Универсальная эквивалентность общих и специальных линейных групп над полями*

Е. И. БУНИНА, Г. А. КАЛЕЕВА
Московский государственный университет им. М. В. Ломоносова
e-mail: helen.bunina@gmail.com

УДК 510.67+512.54.0+512.643

Ключевые слова: универсальная эквивалентность, общие линейные группы, специальные линейные группы.

Аннотация

В данной работе мы доказываем критерий универсальной эквивалентности линейных групп над полями. Доказано, что две полных или специальных линейных группы над полями универсально эквивалентны тогда и только тогда, когда размерности групп совпадают, а поля универсально эквивалентны.

Abstract

E. I. Bunina, G. A. Kaleeva, Universal equivalence of general and special linear groups over fields, Fundamentalnaya i prikladnaya matematika, vol. 21 (2016), no. 3, pp. 73—106.

In this paper, we study universal equivalence of general and special linear groups over fields. We give the following criterion for this relation to hold: two groups $\mathbf{G}_n(K)$ and $\mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$, K and L are infinite fields) are universally equivalent if and only if $n = m$ and the fields K and L are universally equivalent.

1. Введение

Данная работа посвящена изучению универсальных свойств полных и специальных линейных групп.

Впервые проблема связи выразимых в логике первого порядка свойств некоторых моделей со свойствами производных моделей была рассмотрена в 1961 г. в работе А. И. Мальцева [10]. В ней доказана теорема о необходимых и достаточных условиях элементарной эквивалентности линейных групп над полями, а именно: группы $\mathbf{G}_n(K)$ и $\mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}, \mathrm{PGL}, \mathrm{PSL}$, K, L — поля характеристики 0) элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K и L элементарно эквивалентны. В 1992 г. К. И. Бейдар и А. В. Михалёв [15] нашли единый подход к проблемам элементарной эквивалентности

*Исследование выполнено за счёт гранта Российского научного фонда (проект 16-11-10013).

Фундаментальная и прикладная математика, 2016, том 21, № 3, с. 73—106.

общих алгебраических структур и обобщили теорему Мальцева для случая, когда K и L являются телами и ассоциативными кольцами. Продолжением исследований в этой области явились работы Е. И. Буниной 1998—2010 гг. (см. [1—3, 6]), где результаты А. И. Мальцева были распространены на унитарные линейные группы над телами и ассоциативными кольцами с инволюцией, а также на группы Шевалле над полями и локальными кольцами.

Есть и иной путь, по которому может идти изучение вопроса, впервые поставленного Мальцевым, — это рассмотрение других видов эквивалентности. Мы можем обеднить теорию, разрешив использование только одного вида кванторов, и рассматривать алгебраические структуры в рамках этой обеднённой — универсальной — теории. Первые критерии универсальной эквивалентности были установлены Ю. Ш. Гуревичем и А. И. Кокориным [8] для упорядоченных абелевых групп в 1963 г., Н. Г. Хисамиевым [14] для структурно упорядоченных абелевых групп в 1966 г., а затем П. С. Эклофом [16] для произвольных абелевых групп в 1972 г. Позднее другими исследователями были получены результаты об универсальной эквивалентности таких структур, как разрешимые группы (Е. И. Тимошенко [13]), частично коммутативные нильпотентные группы (А. А. Мищенко и Е. И. Тимошенко [17]), частично коммутативные метабелевы алгебры Ли (Е. Н. Порошенко и Е. И. Тимошенко [18]).

Данная работа посвящена универсальной эквивалентности линейных групп над полями. Мы доказываем аналог теоремы Мальцева для универсальной эквивалентности полных и специальных линейных групп над полями, при этом отдельно рассматриваем случаи полей характеристики, отличной от 2, и характеристики 2.

При доказательстве используются критерий универсальной эквивалентности, сформулированный А. Д. Таймановым в статье [12], результаты Е. И. Буниной, А. В. Михалёва, А. Г. Пинуса из книги [7] и метод исследования линейных групп, предложенный О. О'Мирой и изложенный в лекциях [11].

2. Некоторые предварительные сведения

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

$$\forall x_1 \ldots \forall x_n\ \psi(x_1, \ldots, x_n).$$

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

$$\exists x_1 \ldots \exists x_n\ \psi(x_1, \ldots, x_n).$$

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

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

Множество универсальных предложений $\{\varphi \mid \mathfrak{A} \models \varphi\}$ сигнатуры Σ называется *универсальной теорией* системы $\mathfrak{A}$ и обозначается $\mathrm{Th}_{\forall}(\mathfrak{A})$. Таким образом,

$$\mathfrak{A} \equiv_{\forall} \mathfrak{B} \Leftrightarrow \mathrm{Th}_{\forall}(\mathfrak{A}) = \mathrm{Th}_{\forall}(\mathfrak{B}).$$

Замечание 1. Благодаря связи кванторов можно рассматривать экзистенциальную форму записи универсальных формул и $\exists$-теории вместо $\forall$-теорий.

Определение 4. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — алгебраические системы сигнатуры Σ с носителями A и B и f — отображение $A \to B$. Отображение f называется *частичным изоморфизмом* $\mathfrak{A}$ в $\mathfrak{B}$, если выполнены следующие условия:

1) $\mathrm{dom}(f) \subset A$, $\mathrm{Im}(f) \subset B$;
2) f инъективен;
3) f сохраняет предикаты, функции и константы:

   а) для $P^n \in \Sigma$ и $a_0, \ldots, a_{n-1} \in \mathrm{dom}(f)$

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

   б) для $F^n \in \Sigma$ и $a_0, \ldots, a_{n-1}, a \in \mathrm{dom}(f)$

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

   в) для $c \in \Sigma$ и $a \in \mathrm{dom}(f)$

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

Определение 5. Частичный изоморфизм f, у которого область определения конечна, называется *конечным частичным изоморфизмом*.

Теорема 1 (критерий универсальной эквивалентности [12])**.** *Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — системы сигнатуры Σ. Для того чтобы системы $\mathfrak{A}$ и $\mathfrak{B}$ были универсально эквиваленты, необходимо и достаточно, чтобы для любой конечной подсигнатуры $\Sigma_1 \subset \Sigma$ любая конечная подсистема системы $\mathfrak{A}$ сигнатуры Σ_1 была частично изоморфна некоторой подсистеме системы $\mathfrak{B}$ той же сигнатуры и наоборот.*

Данная работа посвящена доказательству следующей теоремы.

Теорема 2. *Пусть K и L — бесконечные поля. Группы $\mathbf{G}_n(K)$ и $\mathbf{G}_m(L)$ $(\mathbf{G} = \mathrm{GL}, \mathrm{SL})$ универсально эквивалентны тогда и только тогда, когда $n = m$ и поля K и L универсально эквивалентны.*

Замечание 2. Если поля K и L конечны, то универсальная эквивалентность совпадает с изоморфизмом и можно сослаться на следующую теорему, изложенную в [11].

Теорема 3. *Пусть n и m — натуральные числа, $n, m \geqslant 2$, 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) $\mathrm{SL}_n(K) \cong \mathrm{SL}_m(L)$.

Сначала докажем более простую импликацию.

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

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

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

$$\mathrm{GL}_n(K) = \Big\{(a_1, \ldots, a_{n^2}) \in K^{n^2} \;\Big|\; \sum_{\sigma \in \mathrm{S}_n} (-1)^\sigma \prod_{i=1}^{n} a_{(i-1)n+\sigma(i)} \neq 0\Big\},$$

$$\mathrm{SL}_n(K) = \Big\{(a_1 \ldots a_{n^2}) \in K^{n^2} \;\Big|\; \sum_{\sigma \in \mathrm{S}_n} (-1)^\sigma \prod_{i=1}^{n} a_{(i-1)n+\sigma(i)} = 1\Big\}.$$

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

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

где

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

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

Предложение доказано. □

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

3. Универсальная эквивалентность линейных групп над полями характеристики 2

В настоящей части работы докажем следующую теорему.

Теорема 4. *Пусть K и L — бесконечные поля характеристики 2, группы $\mathbf{G}_n(K)$ и $\mathbf{G}_m(L)$* ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$) *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 1. *Пусть поле K имеет характеристику 2, $n = 2$ или $n = 3$. Пусть при этом $A \in \mathrm{GL}_n(K)$ ($A \in \mathrm{SL}_n(K)$), $A \neq E$, $A^2 = E$. Тогда в некотором базисе матрица A имеет вид $E + E_{12}$.*

Доказательство. Пусть $V_0 = \mathrm{Ker}(A + E)$ — 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 $(A + E)^2 x = \lambda^2 x = 0$. Учитывая, что $x \neq 0$, получаем, что $\lambda = 0$, 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 $Az + \mu Ax = z + \mu y + \mu x + \mu y = z + \mu x$. Тогда $z + \mu x \in V_0$, значит, $z + \mu x = \nu y$, что противоречит линейной независимости x, y, z. Утверждение доказано. □

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.

3.1. Исследование свойств линейных групп, выражающихся экзистенциальной формулой, в случае когда в поле извлекаются корни третьей степени из единицы

Лемма 2. *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 $\mathrm{diag}[\xi_1, \ldots, \xi_n]$, где все ξ_i — корни третьей степени из единицы.*

Доказательство. Утверждение следует из того, что каждая такая матрица диагонализируема, а также из того, что множество попарно коммутирующих матриц имеет общий собственный вектор. Таким образом, все эти матрицы имеют диагональный вид в общем базисе. □

Обозначим через $\mathcal{A}\big(\mathrm{GL}_n(K)\big)$ ($\mathcal{A}\big(\mathrm{SL}_n(K)\big)$ или просто $\mathcal{A}$, если понятно, о какой группе идёт речь) некоторый фиксированный максимальный набор матриц вида $\mathrm{diag}[\xi_1, \ldots, \xi_n]$, существование которого доказано в лемме 2.

Лемма 3. *Пусть в поле K извлекаются корни третьей степени из единицы и $n \geqslant 4$. Тогда в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ матрица порядка 2, такая что при её сопряжении всеми матрицами из набора $\mathcal{A}$ получаются ровно три различные коммутирующие 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, что $A \neq E$, $A^2 = E$, 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 трёх различных матриц сопряжением — противоречие. Пусть теперь $(p, q) = (s, t)$ и других внедиагональных ненулевых элементов нет. Тогда

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

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:

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

где ξ — неединичный корень третьей степени из 1. Так как любые две из трёх записанных выше матриц коммутируют, то получаем следующее соотношение:

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

Отсюда, 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, порождённую матрицей $E + (a_{ij} + 1)E_{jj}$ (она коммутирует со всеми матрицами из системы $\mathcal{A}$):

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

что и требовалось. □

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

Лемма 5. *Пусть в полях K и L характеристики 2 извлекаются корни третьей степени из единицы и известно, что $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}$ или $\mathbf{G} = \mathrm{SL}$). Тогда $n = m$.*

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

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

утверждающую наличие набора из $3^{N-1} - 1$ попарно различных неединичных попарно коммутирующих матриц порядка 3. Наибольшее значение N, для которого формула (1) истинна в обеих группах, согласно лемме 2 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 (1) истинна в каждой паре групп, выполнено условие $N = m = n$. $\square$

3.2. Исследование свойств линейных групп, выражающихся экзистенциальной формулой, в случае когда в поле не извлекаются корни третьей степени из единицы

Лемма 6. *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 3 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 $3^{[n/2]} - 1$ 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 приёмом, изложенным в [4]. 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 из $x \in K^n$ представи́м 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 $V_1 = \operatorname{Ker} \sigma$. Пусть $x \in V_1$. Тогда $x = (E + \sigma)y$ для некоторого $y \in K^n$. Далее,

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

Из доказанного 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 $\lambda = 1$. Пусть теперь ненулевой вектор x принадлежит 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. Оператор A действует на y следующим образом: $Ay = A^2x = (\sigma + A + E)x = y + x$. Таким образом, подпространство V_1 распадается в прямую сумму двумерных инвариантных подпространств оператора A.

Из доказанного выше следует, что матрица оператора A в некотором базисе имеет блочно-диагональный вид, где на диагонали стоят блоки одного из трёх типов:

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

$\square$

Пусть $\mathcal{B}\big(\mathrm{GL}_n(K)\big)$ $\big(\mathcal{B}\big(\mathrm{SL}_n(K)\big)\big)$ — некоторый фиксированный максимальный набор попарно коммутирующих матриц порядка 3 из леммы 6.

Лемма 7. *Пусть в бесконечном поле K не извлекаются корни третьей степени из единицы и $n > 5$. Тогда в $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ матрица, имеющая в некотором базисе вид $E + E_{12}$, выделяется экзистенциальной формулой.*

Доказательство. Матрицы каждого из наборов $\mathcal{B}\big(\mathrm{GL}_n(K)\big)$ $\big(\mathcal{B}\big(\mathrm{SL}_n(K)\big)\big)$ в соответствующих группах выделяются экзистенциальной формулой: существует $3^{[n/2]}-1$ различных попарно коммутирующих матриц порядка 3. Этот набор матриц разбивается на классы сопряжённости — множества матриц, содержащих одинаковое количество неединичных блоков. Присвоим каждому классу номер, равный количеству неединичных блоков в каждой матрице класса. Таким образом, существует $[n/2]$ классов сопряжённости, в k-м классе $2^k C^k_{[n/2]}$ матриц, $k = 1, \ldots, [n/2]$.

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

Покажем, что не существует биекции классов сопряжённости, не оставляющей на месте первый класс. Достаточно доказать, что $2[n/2] < 2^k C^k_{[n/2]}$ при $1 < k \leqslant [n/2]$. Так как $n > 5$, то $[n/2] > 2$. Тогда при $k = [n/2]$ получим, что $2[n/2] < 1 \cdot 2^{[n/2]}$, а при $1 < k < [n/2]$ получим, что $2[n/2] < 2^k \cdot [n/2] < 2^k \cdot C^k_{[n/2]}$.

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 $A_1, \ldots, A_{[n/2]}$, и пусть $\mathcal{C} = \{A_1, \ldots, A_{[n/2]}\}$. Можем считать, что блоки размерности 2 идут подряд, а номер матрицы равен номеру места, на котором у неё стоит неединичный блок.

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

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

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

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

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

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 $b_{2m-1,i} = b_{2m,i} = 0$, $b_{i,2m-1} = b_{i,2m} = 0$, $i = 1, \dots, \widehat{2m-1}, \widehat{2m}, \dots, n$.

Теперь рассмотрим матрицу C, коммутирующую с $[n/2] - 1$ 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 неё либо $[n/2] = n/2$ блоков размерности 2, либо $[n/2] - 1$ 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, что

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

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

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 1 в некотором базисе (в котором вид матриц системы $\mathcal{B}$, вообще говоря, изменится) матрица C имеет вид $E + E_{12}$. □

Лемма 8. *Пусть в бесконечном поле K не извлекаются корни третьей степени из единицы и $n > 5$. Если n чётно, то в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ ни для какой матрицы из системы $\mathcal{C}$ (определённой в доказательстве леммы 7) не найдётся 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 нечётно, то в группе $\mathrm{SL}_n(K)$ для матрицы из системы $\mathcal{C}$ существуют две такие различные коммутирующие между собой* *матрицы порядка 2 с различными централизаторами, что они коммутируют со всеми матрицами из системы $\mathcal{C}$, кроме данной.*

Доказательство. Если n чётно, то согласно доказательству леммы 7 матрица A_e порядка 2, коммутирующая со всеми, кроме одной (назовём её B_e и будем считать, что у неё 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 $\mathcal{C}$. 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

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

но централизатор каждой такой матрицы совпадает с централизатором матрицы A_e.

Пусть теперь n нечётно. Тогда согласно лемме 7 матрица A_o порядка 2, коммутирующая со всеми, кроме одной (назовём её 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):

$$\begin{pmatrix} 1 & 1 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 1 & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}.$$

Лемма доказана. □

Прежде чем доказывать лемму, аналогичную лемме 5, 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 $2 \leqslant n \leqslant 5$.

При $n = 2$ в группах $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ максимальный набор из 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 из попарно коммутирующих матриц порядка 3 также состоит из двух матриц, но найдутся две 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 восьми 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 имеет жорданова клетка размерности 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 9. *Пусть в бесконечных полях K и L характеристики 2 не извлекаются корни третьей степени из единицы и известно, что $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}$ или $\mathbf{G} = \mathrm{SL}$). Тогда $n = m$.*

Доказательство. Рассмотрим формулу

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

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 $\mathbf{G}_n(K)$ и $\mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL4}$), одинаково, и согласно лемме 8 $N = [n/2] = [m/2]$.

Если $N = 1$, то формула

$$\exists A_1 \ \exists A_2 \ \exists C \ \big((\neg A_1 = A_2) \mathbin{\&} (\neg A_1 = E) \mathbin{\&} (\neg A_2 = E) \mathbin{\&}$$
$$\mathbin{\&} (A_1A_2 = A_2A_1) \mathbin{\&} (A_1^2 = E) \mathbin{\&} (A_2^2 = E) \mathbin{\&}$$
$$\mathbin{\&} (A_1C = CA_1) \mathbin{\&} (\neg A_2C = CA_2)\big),$$

утверждающая наличие в группе двух различных коммутирующих матриц порядка 2, имеющих различные централизаторы, либо истинна, либо ложна одновременно 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

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

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

Пусть теперь $N \geqslant 3$. Значит, $n, m \geqslant 6$, и мы можем использовать приёмы из лемм 7 и 8. Рассмотрим формулу

$$\exists A_{11} \ \ldots \ \exists A_{1,2C_M^1} \ \exists A_{21} \ \ldots \ \exists A_{2,2^2C_M^2} \ \ldots \ \exists A_{M,1} \ \ldots \ \exists A_{M,2^MC_M^M}$$
$$\exists B_1 \ \exists B_2 \ \exists C \ \exists C_{k,i,j} \ (k = 1, \ldots, M; \ i,j = 1, \ldots, k)$$
$$\left(\bigwedge_{k=1}^{M} \bigwedge_{i=1}^{2^kC_M^k} (\neg A_{k,i} = E) \mathbin{\&} \bigwedge_{k=1}^{M} \bigwedge_{i=1}^{2^kC_M^k} \bigwedge_{l=1}^{M} \bigwedge_{\substack{j=1\\ (k,i)\neq(l,j)}}^{2^lC_M^l} (\neg A_{k,i} = A_{l,j}) \mathbin{\&} \right.$$
$$\mathbin{\&} \bigwedge_{k=1}^{M} \bigwedge_{i=1}^{2^kC_M^k} \bigwedge_{l=1}^{M} \bigwedge_{j=1}^{2^lC_M^l} (A_{k,i}A_{l,j} = A_{l,j}A_{k,i}) \mathbin{\&} \bigwedge_{k=1}^{M} \bigwedge_{i=1}^{2^kC_M^k} (A_{k,i}^3 = E) \mathbin{\&}$$
$$\mathbin{\&} \bigwedge_{k=1}^{M} \bigwedge_{i=1}^{2^kC_M^k} \bigwedge_{j=1}^{2^kC_M^k} (A_{k,i} = C_{k,i,j}^{-1}A_{k,j}C_{k,i,j}) \mathbin{\&} \bigwedge_{i=1}^{C_M^1} (A_{1,i}A_{1,i+C_M^1} = E) \mathbin{\&}$$

$$
\begin{aligned}
&\& (\neg B_1 = E) \;\&\; (\neg B_2 = E) \;\& \\
&\& \bigwedge_{i=1}^{C_M^1-1} (B_1 A_{1,i} = A_{1,i} B_1) \;\&\; \bigwedge_{i=1}^{C_M^1-1} (B_2 A_{1,i} = A_{1,i} B_2) \;\& \\
&\& (B_1^2 = E) \;\&\; (B_2^2 = E) \;\&\; (B_1 B_2 = B_2 B_1) \;\& \\
&\& (B_1 C = C B_1) \;\&\; (\neg B_2 C = C B_2)\Big).
\end{aligned}
$$

При M, равном целой части от половины размерности группы, эта формула выделяет среди матриц системы $\mathcal{B}$ класс сопряжённости, состоящий из матриц, имеющих ровно один неединичный блок (это $A_{11}, \ldots, A_{1,2C_M^1}$), и систему $\mathcal{C}$ среди них, $\mathcal{C} = \{A_{11}, \ldots, A_{1,C_M^1}\}$. 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 $n = m = 2M$. □

3.3. Исследование свойств линейных групп, выражающихся экзистенциальной формулой, без предположения о наличии корней третьей степени из единицы

Предложение 2. *Пусть бесконечные поля K и L имеют характеристику 2 и* $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}$ *или* $\mathbf{G} = \mathrm{SL}$). *Тогда* $n = m$.

Доказательство. Выпишем две формулы:

$$
\begin{aligned}
\exists A_1 \ \ldots\ \exists A_{3^N-1} \Bigg(&\bigwedge_{i=1}^{3^N-1} (\neg A_i = E) \;\&\; \bigwedge_{\substack{i,j=1\\ i\neq j}}^{3^N-1} (\neg A_i = A_j) \;\& \\
&\& \bigwedge_{i,j=1}^{3^N-1} (A_i A_j = A_j A_i) \;\&\; \bigwedge_{i=1}^{3^N-1} (A_i^3 = E)\Bigg),
\end{aligned}
\tag{2}
$$

$$
\exists J \left(\bigwedge_{i=1}^{2^k-1} (\neg J^i = E) \;\&\; (J^{2^k} = E)\right). \tag{3}
$$

Так как группы универсально эквивалентны, то наибольшее N, для которого истинна формула (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 (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 $2^k \geqslant n$, $2^k \geqslant m$, получаем, что

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

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 $n = m$ совпадает с этим числом. Мы также узнаём, 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 9 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 $\mathrm{SL}_{N+1}(K)$ 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 найдётся 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 не коммутирующие друг с другом матрицы

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

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 $N > 2$ выполнено $2N - (N+1) \geqslant 2$, и привести пример двух некоммутирующих матриц из централизатора жордановой клетки порядка 2^k также нетрудно. □

Определение 6. Назовём конечный частичный изоморфизм

$$\Phi\colon \mathbf{G}_n(K) \to \mathbf{G}_m(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL})$$

особым, если $\mathrm{dom}(\Phi)$ 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 $E + E_{ij}$ $(i, j = 1, \ldots, n;\ i \neq j)$ в соответствующем базисе, а также вспомогательные матрицы из формул, использованных при доказательстве леммы 9 и предложения 2 (их конечное число).

Лемма 10. *Пусть бесконечные поля K и L имеют характеристику 2 и известно, что $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_m(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$). Тогда при любом особом конечном частичном изоморфизме*

$$\Phi\colon \mathbf{G}_n(K) \to \mathbf{G}_m(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL})$$

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 1.

Пусть теперь $n = m \geqslant 4$. 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 3, а если корни не извлекаются и $n = m \geqslant 6$, то из леммы 7. 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

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

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. Её четвёртая 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 результатами из [5], а именно леммами 2.20 и 2.21.

Лемма 11. *Пусть бесконечные поля K и L имеют характеристику 2 и известно, что $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_n(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$). Тогда при любом особом конечном частичном изоморфизме*

$$\Phi\colon \mathbf{G}_n(K) \to \mathbf{G}_m(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL})$$

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

3.4. Доказательство основной теоремы

Определение 7. Для данного элемента α поля K матрицу $E+\alpha E_{12} \in \in \mathrm{GL}_n(K)$ ($E+\alpha E_{12} \in \mathrm{SL}_n(K)$) назовём *матрицей сложения*, а матрицу $\mathrm{diag}[\alpha, 1/\alpha, 1, \ldots, 1]$ — *матрицей умножения*.

Лемма 12. *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. □

Лемма 13. *Пусть бесконечные поля K и L имеют характеристику 2 и*

$$\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_m(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL}).$$

Тогда при любом особом конечном частичном изоморфизме

$$\Phi\colon \mathbf{G}_n(K) \to \mathbf{G}_m(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL})$$

матрицы сложения и умножения переходят в матрицы того же вида, причём если

$$\Phi\left(\alpha E_{11} + \frac{1}{\alpha} E_{22}\right) = \beta E_{11} + \frac{1}{\beta}$$

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 матриц (a_{st}), у которых $a_{si}=0$, $1 \leqslant s \leqslant n$, $s \neq i$, $a_{jt}=0$, $1 \leqslant t \leqslant n$, $t \neq i$, $a_{ii}=a_{jj}$. 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:

$$\begin{gathered} A(E+E_{ij}) = (E+E_{ij})A \quad (3 \leqslant i \leqslant n,\ 3 \leqslant j \leqslant n,\ i \neq j), \\ (A(E+E_{12})A^{-1})(E+E_{12}) = (E+E_{12})(A(E+E_{12})A^{-1}), \\ (A(E+E_{21})A^{-1})(E+E_{21}) = (E+E_{21})(A(E+E_{21})A^{-1}), \\ \big((E+E_{12})(E+E_{21})(E+E_{12})A\big)^2 = E. \end{gathered}$$

Из первого условия следует, что

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

Далее,

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

$$\times \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1 \end{pmatrix} \begin{pmatrix} a_{22} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{11} & 0 & \dots & 0 \\ 0 & 0 & 1/\lambda & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1/\lambda \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ 0 & 0 & \lambda & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda \end{pmatrix} \begin{pmatrix} a_{21}+a_{22} & a_{11}+a_{12} & 0 & \dots & 0 \\ a_{21} & a_{11} & 0 & \dots & 0 \\ 0 & 0 & 1/\lambda & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1/\lambda \end{pmatrix} =$$

$$= \begin{pmatrix} * & * & 0 & \dots & 0 \\ a_{21}^2 & * & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1 \end{pmatrix}$$

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

Теперь применим последнее соотношение. Так как

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

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

Теперь докажем второе утверждение леммы. Пусть

$$\Phi\left(E+\frac{1}{\alpha}E_{21}\right) = E+\delta E_{21}$$

(то, что вид сохраняется, доказывается аналогично сохранению вида $E+\alpha E_{12}$). В $\mathrm{GL}_n(K)$ ($\mathrm{SL}_n(K)$) выполнено следующее соотношение:

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

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

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

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

Доказательство теоремы 4. 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 подмодель поля K. Наша задача — найти для неё конечно частично изоморфную ей подмодель L_1 в поле L. Пусть $G_1\subset \mathbf{G}_n(K)$ ($\mathbf{G}=\mathrm{GL},\mathrm{SL}$) содержит все матрицы сложения $E+\alpha E_{12}$ и умножения $\mathrm{diag}[\alpha,1/\alpha,1,\ldots,1]$ 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 $E+E_{ij}$ ($i,j=1,\ldots,n$, $i\neq j$) и конечное число вспомогательных матриц из лемм 5, 9 и предложения 2. Так как группы универсально эквивалентны, то для подмодели G_1 существует конечная подмодель $G_2\subset\mathbf{G}_n(K)$ ($\mathbf{G}=\mathrm{GL},\mathrm{SL}$), частично изоморфная G_1, причём конечный частичный изоморфизм $\Phi\colon G_1\to G_2$ является особым. Поэтому матрицы сложения и умножения переходят в матрицы того же вида, и если матрицы сложения S и 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. □

4. Универсальная эквивалентность линейных групп над полями характеристики, отличной от 2

В этом разделе мы докажем следующую теорему.

Теорема 5. *Пусть K и L — бесконечные поля, $\mathrm{char}\,K,\mathrm{char}\,L\neq 2$, группы $\mathbf{G}_n(K)$ и $\mathbf{G}_m(L)$ ($\mathbf{G}=\mathrm{GL},\mathrm{SL}$) 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.

4.1. Свойства линейных групп, выражающиеся экзистенциальной формулой

Лемма 14. *Пусть K — поле, $\operatorname{char} K \neq 2$, n — натуральное число. В группе $\mathrm{GL}_n(K)$ существует подмножество максимум из $2^n - 1$ попарно коммутирующих матриц порядка 2, а в группе $\mathrm{SL}_n(K)$ — из $2^{n-1} - 1$ попарно коммутирующих матриц порядка 2.*

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

Обозначим через $\mathcal{D}(\mathrm{GL}_n(K))$ $(\mathcal{D}(\mathrm{SL}_n(K))$ или просто $\mathcal{D}$, если понятно, о какой группе идёт речь) некоторый фиксированный максимальный набор попарно коммутирующих матриц порядка 2, существование которого доказано в лемме 14. Ясно, что набор матриц $\mathcal{D}$ выделяется экзистенциальной формулой.

Заметим, что благодаря лемме 14 мы можем разделить случаи, когда поля имеют характеристику 2 и характеристику, отличную от 2. Действительно, справедлива следующая лемма.

Лемма 15. *Пусть K и L — бесконечные поля произвольной характеристики, группы $\mathbf{G}_n(K)$ и $\mathbf{G}_m(L)$ $(\mathbf{G} = \mathrm{GL}, \mathrm{SL})$ универсально эквивалентны. Тогда либо $\operatorname{char} K = \operatorname{char} L = 2$, либо $\operatorname{char} K \neq 2$ и $\operatorname{char} L \neq 2$.*

Доказательство. Запишем следующую формулу:

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

Если для некоторого достаточно большого M она ложна в обеих группах, то характеристика обоих полей отлична от 2. В противном случае характеристика полей равна 2. Действительно, так как поле бесконечно, то для любого сколь угодно большого M набор матриц вида $E + \alpha_i E_{12}$, где $\alpha_1, \ldots, \alpha_M$ — различные элементы поля, можно взять в качестве $A_1, \ldots, A_M$. $\square$

Все попарно коммутирующие инволюции из системы $\mathcal{D}$ разбиваются на классы сопряжённости, 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 $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_m(L)$ $(\mathbf{G} = \mathrm{GL}, \mathrm{SL})$. Тогда $n = m$.*

Доказательство. Рассмотрим формулу

$$\exists A_1 \ \ldots \ \exists A_{2^N-1} \left(\bigwedge_{i=1}^{2^N-1} (\neg A_i = E) \ \& \bigwedge_{\substack{i,j=1 \\ i\neq j}}^{2^N-1} (\neg A_i = A_j) \ \& \right.$$
$$\left. \& \bigwedge_{i,j=1}^{2^N-1} (A_iA_j = A_jA_i) \ \& \bigwedge_{i=1}^{2^N-1} (A_i^2 = E) \right). \quad (4)$$

Так как группы универсально эквивалентны, то наибольшее N, такое что формула (4) истинна в группах, одинаково для обеих групп. В случае общих линейных групп $n = m = N$, а в случае специальных линейных групп $n = m = N + 1$. □

Лемма 16. *Пусть K — бесконечное поле, $\mathrm{char}\, K \neq 2$. В группе $\mathrm{GL}_n(K)$ два подмножества системы $\mathcal{D}$, состоящие из матриц, у которых -1 на диагонали встречается один или $n-1$ раз, выделяются экзистенциальной формулой. Если n нечётно, то в группе $\mathrm{SL}_n(K)$ 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 $\mathrm{GL}_n(K)$ в двух классах сопряжённости, содержащих по n элементов, а в $\mathrm{SL}_n(K)$ — в одном n-элементном классе сопряжённости; во всех остальных классах сопряжённости (кроме класса, состоящего из одной матрицы $-E$, в случае $\mathrm{GL}_n(K)$) инволюций больше. □

Определение 8. Обозначим через $\mathcal{E}$ подмножество матриц системы $\mathcal{D}$, у которых -1 стоит на диагонали один или $n-1$ раз. Согласно предыдущей лемме такое множество матриц выделяется экзистенциальной формулой.

Лемма 17. *Пусть бесконечные поля K и L имеют характеристику, отличную от 2, и известно, что $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_n(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$), а также n нечётно в случае специальных линейных групп. Тогда при любом конечном частичном изоморфизме*

$$\Phi\colon \mathbf{G}_n(K) \to \mathbf{G}_n(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL}),$$

таком что $\mathrm{dom}\,\Phi$ 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 её образ, следовательно, образ является диагональной матрицей. □

Лемма 18. *Пусть бесконечные поля K и L имеют характеристику, отличную от 2, и известно, что $\mathbf{G}_n(K) \equiv_\forall \mathbf{G}_n(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$, n нечётно для специальных линейных групп). Тогда при любом конечном частичном изоморфизме*

$$\Phi\colon \mathbf{G}_n(K) \to \mathbf{G}_n(L) \quad (\mathbf{G} = \mathrm{GL}, \mathrm{SL}),$$

таком что $\operatorname{dom}\Phi$ *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*

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \pm1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \pm1 \end{pmatrix}$$

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 матрицами системы $\mathcal{E}$, кроме двух. 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 $\mathcal{D}$ -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 $d_{22}^2 = 1$ и $-d_{22}^2 = 1$ — противоречие. Отсюда следует, что $d_{22} = 0$. Из того, что $d_{12}d_{21} + d_{22}^2 = 1$, получим, что $d_{12}d_{21} = 1$, следовательно, $d_{11} = 0$. Таким образом, образ матрицы $-E + E_{11} + E_{22} + E_{21} + E_{12}$ имеет вид

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

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

Лемма 19. *Пусть K, L — бесконечные поля,* $\operatorname{char} K, \operatorname{char} L \neq 2$. *При любом конечном частичном изоморфизме между группами $\mathbf{G}_n(K)$ и $\mathbf{G}_n(L)$* ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$ *и n нечётно в случае специальных линейных групп*), *область которого содержит все попарно коммутирующие инволюции, матрицу $-E+E_{11}+$ $+E_{22}+E_{12}+E_{21}$, матрицу* $\operatorname{diag}[2, 1, 1/2, 1, \dots, 1]$ (*матрицу* $\operatorname{diag}[2, 1]$ *при* $\mathbf{G} = \mathrm{GL}$ *и* $n = 2$), *а также конечный набор вспомогательных матриц, матрицы вида $E + \alpha_i E_{12}$, $i = 1, \dots, k$, отображаются 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 $E_{12}+E_{21}+\operatorname{diag}[0, 0, \pm 1, \dots, \pm 1]$, а диагональные матрицы — в диагональные.

Теперь перейдём 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, её 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: $\operatorname{char} K = 3$ и $\operatorname{char} K \neq 3$.

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

Возьмём 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 $\mathrm{diag}[\pm 1, \ldots, \pm 1]$, у которой на диагонали -1 встречается ровно два 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 следующие соотношения:

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

$$= \frac{\lambda_3 \cdots \lambda_n}{ad - bc} \begin{pmatrix} d & -b & 0 & \ldots & 0 \\ -c & a & 0 & \ldots & 0 \\ 0 & 0 & \lambda_3 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \lambda_n \end{pmatrix}.$$

Из первого равенства получаем, что $\lambda_3 = \ldots = \lambda_n = 1$. А так как b и c одновременно не равны 0 (иначе образ матрицы $E + \alpha E_{12}$ коммутирует со всеми матрицами системы $\mathcal{E}$, что неверно), то из $-b = -b/(ad - bc)$ или $-c = -c/(ad - bc)$ получаем, что $ad - bc = 1$. 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 $\mathrm{char}\, K = 3$ утверждение доказано.

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

$$(\mathrm{diag}[2, 1, 1/2, 1, \ldots, 1])(E + \alpha E_{12})(\mathrm{diag}[2, 1, 1/2, 1, \ldots, 1])^{-1} = (E + \alpha E_{12})^2.$$

Образ матрицы $\mathrm{diag}[2, 1, 1/2, 1, \ldots, 1]$ при конечном частичном изоморфизме равен некоторой диагональной матрице $\mathrm{diag}[\alpha_1, \ldots, \alpha_n]$, причём из того, что матрица $(\mathrm{diag}[2, 1, 1/2, 1, \ldots, 1])^2$ не коммутирует с $-E + E_{11} + E_{12} + E_{21} + E_{22}$, следует, что $(\mathrm{diag}[\alpha_1, \ldots, \alpha_n])^2$ 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:

$$\begin{pmatrix} a & b\alpha_1/\alpha_2 & 0 & \ldots & 0 \\ c\alpha_2/\alpha_1 & d & 0 & \ldots & 0 \\ 0 & 0 & \lambda_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix} =$$

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

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

Отсюда получаем, что $\lambda_i = 1$, $i = 3, \dots, n$. Если $bc \neq 0$, то, так как

$$\frac{b\alpha_1}{\alpha_2} = b(a+d)$$

и

$$\frac{c\alpha_2}{\alpha_1} = c(a+d),$$

имеем

$$\frac{\alpha_1}{\alpha_2} = a + d = \frac{\alpha_2}{\alpha_1},$$

следовательно, $\alpha_1^2 = \alpha_2^2$, что противоречит ранее доказанному. Значит, $bc = 0$ и $a = d = 1$. □

Лемма 20. *Пусть K, L — бесконечные поля, $\operatorname{char} K, \operatorname{char} L \neq 2$. При любом конечном частичном изоморфизме между группами $\mathbf{G}_n(K)$ и $\mathbf{G}_n(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}_n(K)$, n нечётно в случае специальных линейных групп), область которого содержит все попарно коммутирующие инволюции, матрицу $-E + E_{11} + E_{12} + E_{21} + E_{22}$, матрицу $\operatorname{diag}[2, 1, 1/2, 1, \dots, 1]$ ($\operatorname{diag}[2, 1]$ в случае $\mathbf{G} = \mathrm{GL}$, $n = 2$) и конечный набор вспомогательных матриц из предыдущих лемм, матрица $E + E_{12}$ отобразится в матрицу $E + E_{12}$.*

Доказательство. Ранее было 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

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

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

Лемма 21. *Пусть K, L — бесконечные поля, $\operatorname{char} K, \operatorname{char} L \neq 2$. При любом конечном частичном изоморфизме между группами $\mathbf{G}_n(K)$ и $\mathbf{G}_n(L)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}$, n нечётно в случае $\mathbf{G} = \mathrm{SL}$), область которого содержит конечный набор матриц, использованных для доказательства предыдущих лемм, матрицы сложения переходят в матрицы сложения, а матрицы умножения переходят в матрицы умножения, причём 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):

$$\begin{pmatrix}\alpha & 0\\ 0 & 1/\alpha\end{pmatrix} = \begin{pmatrix}1 & -\alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 1/\alpha & 1\end{pmatrix}\begin{pmatrix}1 & -\alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \\ = \begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}^{-1}\left[\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1/\alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right]\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}^{-1}\times \\ \times\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\left[\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right]\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Тогда угловой блок образа рассматриваемой матрицы умножения (диагональная матрица со всеми, кроме первых двух, единичными элементами на диагонали) будет равен произведению

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

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. □

Лемма 22. *Пусть K — бесконечное поле, $\operatorname{char} K \neq 2$. Тогда в группе $\mathrm{SL}_2(K)$ матрица, имеющая в некотором базисе вид $E+E_{12}$, выделяется экзистенциальной формулой.*

Доказательство. Докажем, что матрица A, удовлетворяющая формуле

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

в некотором базисе имеет требуемый вид.

Заметим, что для матрицы $A = E + E_{12}$ формула истинна при

$$X = \alpha E_{11} + \frac{1}{\alpha}E_{22}, \quad \alpha \in K, \quad \alpha \neq \pm 1, \quad Y = 2E_{11} + \frac{1}{2}E_{22}.$$

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

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

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

Если матрица A диагонализируема над $\bar{K}$, то диагональная форма имеет вид $\alpha E_{11} + 1/\alpha$, причём $\alpha \neq \pm 1$, так как $A^2 \neq E$. Введём обозначение

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

и запишем соотношения из нашей формулы:

$$XAX^{-1}A = \begin{pmatrix} \alpha a & b/\alpha \\ c\alpha & d/\alpha \end{pmatrix} \begin{pmatrix} \alpha d & -b/\alpha \\ -c\alpha & a/\alpha \end{pmatrix} = \begin{pmatrix} ad\alpha^2 - bc & -ab + ab/\alpha^2 \\ cd\alpha^2 - cd & -bc + ad/\alpha^2 \end{pmatrix} =$$
$$= \begin{pmatrix} ad\alpha^2 - bc & ab - ab\alpha^2 \\ -cd/\alpha^2 + cd & -bc + ad/\alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ c/\alpha & d/\alpha \end{pmatrix} \begin{pmatrix} \alpha d & -\alpha b \\ -c/\alpha & a/\alpha \end{pmatrix} = AXAX^{-1},$$

$$X^2A = \begin{pmatrix} (a^2+bc)\alpha & (ab+bd)/\alpha \\ (ac+cd)\alpha & (bc+d^2)/\alpha \end{pmatrix} \neq \begin{pmatrix} (a^2+bc)\alpha & (ab+bd)\alpha \\ (ac+cd)/\alpha & (bc+d^2)/\alpha \end{pmatrix} = AX^2.$$

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

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

а так как $\alpha \neq \pm 1$, то $ab = cd = 0$. Но тогда

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

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

Лемма 23. *Пусть K — бесконечное поле, $\operatorname{char} K \neq 2$. Тогда в группе $\mathrm{SL}_2(K)$ 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:

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

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

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

Пусть

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

Из записанных выше соотношений получим, что

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

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

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

является единичной матрицей только при $\operatorname{char} K=3$. 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, что $c=1$. Если $a=0$, то, так как $B\in \mathrm{SL}_2(K)$, $b=-1$, и утверждение доказано. В противном случае сделаем замену базиса, порождённую матрицей $E-aE_{12}$ (коммутирует с $E+E_{12}$), которая приведёт B к виду

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

что и требовалось. □

Лемма 24. *Пусть K — бесконечное поле, $\operatorname{char} K \neq 2$. Тогда в группе $\mathrm{SL}_2(K)$ матрица, имеющая вид $\operatorname{diag}[\alpha, 1/\alpha]$ 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: $(\operatorname{diag}[\alpha, 1/\alpha])(E+E_{12})(\operatorname{diag}[\alpha, 1/\alpha])^{-1}$ коммутирует с $E+E_{12}$, $(-E_{12}+E_{21})(\operatorname{diag}[\alpha, 1/\alpha]) = (\operatorname{diag}[\alpha, 1/\alpha])^{-1}(-E_{12}+E_{21})$.

Пусть некотрая 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,

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

значит, $b=0$, и рассматриваемая матрица диагональна. □

Лемма 25. *Пусть K, L — бесконечные поля, $\operatorname{char} K, \operatorname{char} L \neq 2$. При любом конечном частичном изоморфизме между группами $\mathrm{SL}_2(K)$ и $\mathrm{SL}_2(L)$, область которого содержит набор матриц, использованных при доказательстве предыдущих лемм, матрицы сложения переходят в матрицы сложения, а матрицы умножения переходят в матрицы умножения, причём 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, её образ будет иметь вид $\pm E+\beta E_{12}$. Так как

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

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

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

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 21, если заметить, что
$$\begin{pmatrix} 1 & 0 \\ 1/\alpha & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -1/\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \qquad \square$$

Лемма 26. *Пусть K — бесконечное поле, $\operatorname{char} K \neq 2$, $n \geqslant 4$, n чётно. 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 сопряжённости. Подмножества, состоящие из матриц, имеющих $n-2$ или две -1 на диагонали — это два класса сопряжённости, состоящие из C_n^2 элементов каждый. В остальных классах сопряжённости, кроме класса, состоящего из единственного элемента $-E$, элементов больше. Если $n = 4$, то класс сопряжённости, состоящий из C_n^2, единственный, он является интересующим нас подмножеством.

Если $n = 6$, то, перемножив все элементы из класса сопряжённости 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 сопряжённости, содержащего матрицы с четырьмя -1, то получится единичная матрица, так как среди матриц этого класса сопряжённости 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 два раза.

Если $n \geqslant 8$, 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 сопряжённости. $\square$

Лемма 27. *Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n чётно, $n \geqslant 4$ и известно, что $\mathrm{SL}_n(K) \equiv_\forall \mathrm{SL}_n(L)$. Тогда при любом таком конечном частичном изоморфизме $\Phi\colon \mathrm{SL}_n(K) \to \mathrm{SL}_n(L)$, что $\operatorname{dom}\Phi$ содержит все матрицы системы $\mathcal{D}$, диагональная матрица отображается в диагональную матрицу.*

Доказательство. Из предложения 3 следует, что $n = m$. Так как диагональная матрица коммутирует со всеми матрицами системы $\mathcal{D}$, то и её 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. □

Лемма 28. *Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n чётно, $n \geqslant 4$ и известно, что $\mathrm{SL}_n(K) \equiv_\forall \mathrm{SL}_n(L)$. Тогда при любом таком конечном частичном изоморфизме $\Phi\colon \mathrm{SL}_n(K) \to \mathrm{SL}_n(L)$, что $\mathrm{dom}\,\Phi$ 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. Введём 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-м и j-м 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 сопряжённую 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 её образа. Обозначим образ X. Тогда

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

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

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} даёт матрицу с двумя -1, и назовём её A_{13}. Тогда $A_{23} = A_{12}A_{13}$. Для образов справедливо соотношение (запишем его только 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 $ad-bc=\pm1$. 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, что $a = d = 0$. Сделав замену базиса при помощи матрицы $E + (-1 - 1/b)E_{11}$, 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

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

т. е. $X^2 = E$, что противоречит условию $X^2 = A_{12}$. □

Лемма 29. *Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n чётно, $n \geqslant 4$ и известно, что $\mathrm{SL}_n(K) \equiv_\forall \mathrm{SL}_n(L)$. Тогда при любом таком конечном частичном изоморфизме $\Phi\colon \mathrm{SL}_n(K) \to \mathrm{SL}_n(L)$, что $\operatorname{dom}\Phi$ содержит все матрицы системы $\mathcal{D}$, матрицу $E - E_{11} - E_{22} - E_{12} + E_{21}$ и матрицу $\operatorname{diag}[2, 1, 1/2, 1, \ldots, 1]$, 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 19, если учесть, что роль матрицы $-E+E_{11}+E_{12}+E_{21}+E_{22}$ в данном случае играет матрица $E - E_{11} - E_{22} - E_{12} + E_{21}$. □

Лемма 30. *Пусть бесконечные поля K и L имеют характеристику, отличную от 2, n чётно, $n \geqslant 4$ и известно, что $\mathrm{SL}_n(K) \equiv_\forall \mathrm{SL}_n(L)$. Тогда для любого такого конечного частичного изоморфизма $\Phi\colon \mathrm{SL}_n(K) \to \mathrm{SL}_n(L)$, что $\operatorname{dom}\Phi$ содержит все матрицы системы $\mathcal{D}$, матрицу $E - E_{11} - E_{22} - E_{12} + E_{21}$ и матрицу $\operatorname{diag}[2, 1, 1/2, 1, \ldots, 1]$, а также конечный набор вспомогательных матриц из предыдущих лемм, верно, что $\Phi(E + E_{12}) = E + E_{12}$.*

Доказательство. Так как выполняется 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 учётом 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, что $\alpha = 1$, что и требовалось. $\square$

Для завершения доказательства основной теоремы 2 воспользуемся соображениями, изложенными ранее. Более подробно, мы уже умеем доказывать сохранение вида матриц сложения чётного 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, причём сохраняется соответствие пары матриц сложения и умножения одному элементу поля, полностью аналогично доказательству леммы 21 с учётом замечания из доказательства леммы 25. Теперь остаётся только почти дословно повторить рассуждение из доказательства теоремы 4 в условии теоремы 5. Так как благодаря лемме 15 мы можем различить случаи, в которых основные поля имеют характеристику 2 и характеристику, отличную от 2, то теорема 2 полностью доказана.

Литература

[1] Бунина Е. И. Элементарная эквивалентность унитарных линейных групп над кольцами и телами // УМН. — 1998. — Т. 53, № 2. — С. 137—138.

[2] Бунина Е. И. Элементарная эквивалентность унитарных линейных групп над полями // Фундамент. и прикл. матем. — 1998. — Т. 4, вып. 4. — С. 1265—1278.

[3] Бунина Е. И. Элементарная эквивалентность групп Шевалле // УМН. — 2001. — Т. 56, № 1. — С. 157—158.

[4] Бунина Е. И. Автоморфизмы групп Шевалле типов A_l, D_l, E_l над локальными кольцами с необратимой двойкой // Фундамент. и прикл. матем. — 2009. — Т. 15, № 7. — С. 47—80.

[5] Бунина Е. И. Применение метода локализации для описания автоморфизмов линейных групп над коммутативными кольцами. — 2010. — `http://halgebra.math.msu.su/wiki/lib/exe/fetch.php/specialcourses:speckurs10.pdf`.

[6] Бунина Е. И. Элементарная эквивалентность групп Шевалле над локальными кольцами // Матем. сб. — 2010. — Т. 201, № 3. — С. 3—20.

[7] Бунина Е. И., Михалёв А. В., Пинус А. Г. Элементарная и близкие к ней логические эквивалентности классических и универсальных алгебр. — М.: МЦНМО, 2015.

[8] Гуревич Ю. Ш., Кокорин А. И. Универсальная эквивалентность упорядоченных абелевых групп // Алгебра и логика. — 1963. — Т. 2, № 1. — С. 37—39.

[9] Ершов Ю. Л., Палютин Е. А. Математическая логика. — М.: Наука, 1987.

[10] Мальцев А. И. Об элементарных свойствах линейных групп // Проблемы математики и механики. — Новосибирск, 1961. — С. 110—132.

[11] О'Мира О. Лекции о линейных группах // Автоморфизмы классических групп. — М.: Мир, 1976. — С. 57—167.

[12] Тайманов А. Д. Характеристики аксиоматизируемых классов моделей // Алгебра и логика. — 1962. — Т. 1, № 4. — С. 5—31.

[13] Тимошенко Е. И. Об универсально эквивалентных разрешимых группах // Алгебра и логика. — 2000. — Т. 39, № 2. — С. 227—240.

[14] Хисамиев Н. Г. Универсальная теория структурно упорядоченных абелевых групп // Алгебра и логика. — 1966. — Т. 5, № 3. — С. 71—76.

[15] Beidar C. I., Mikhalev A. V. On Mal'cev's theorem on elementary equivalence of linear groups // Proc. of the Int. Conf. on Algebra Dedicated to the Memory of A. I. Malcev (Novosibirsk, 1989) / L. A. Bokut', A. I. Mal'cev, A. I. Kostrikin, eds. — Amer. Math. Soc., 1992. — (Contemp. Math.; Vol. 131). — P. 29—35.

[16] Eklof P. C. Some model theory for Abelian groups // J. Symb. Logic. — 1972. — Vol. 37. — P. 335—342.

[17] Mishchenko A. A., Timoshenko E. I. Universal equivalence of partially commutative nilpotent groups // Sib. Math. J. — 2011. — Vol. 52, no. 5. — P. 884—891.

[18] Poroshenko E. N., Timoshenko E. I. Universal equivalence of partially commutative metabelian Lie algebras // J. Algebra. — 2013. — Vol. 384. — P. 143—168.