Универсальная эквивалентность симплектических групп

Е. И. БУНИНА
Московский государственный университет
им. М. В. Ломоносова
e-mail: helenbunina@gmail.com

А. М. ЛАЗАРЕВ
Московский государственный университет
им. М. В. Ломоносова

УДК 510.67+512.54.0+512.643

Ключевые слова: универсальная эквивалентность, симплектические линейные группы.

Аннотация

В работе доказан критерий универсальной эквивалентности симплектических линейных групп над полями: две симплектические линейные группы $\mathrm{Sp}_{2n}(K)$ и $\mathrm{Sp}_{2m}(M)$, где $n, m \geqslant 1$, K, M — бесконечные поля характеристики, отличной от двух, универсально эквивалентны тогда и только тогда, когда $n = m$, а поля K и M универсально эквивалентны.

Abstract

E. I. Bunina, A. M. Lazarev, Universal equivalence of symplectic groups, Fundamentalnaya i prikladnaya matematika, vol. 23 (2021), no. 4, pp. 17—38.

In this paper, we prove a criterion of universal equivalence of symplectic linear groups over fields: two symplectic linear groups $\mathrm{Sp}_{2n}(K)$ and $\mathrm{Sp}_{2m}(M)$, where $n, m \geqslant 1$ and K and M are infinite fields of characteristic not equal to 2, are universally equivalent if and only if $n = m$ and the fields K and M are universally equivalent.

1. Введение

Проблема связи выразимых в логике первого порядка свойств некоторых моделей со свойствами производных моделей впервые была рассмотрена в 1961 г. в работе А. И. Мальцева «Об элементарных свойствах линейных групп» [10]. Там доказана теорема о необходимых и достаточных условиях элементарной эквивалентности линейных групп над полями, а именно: группы $\mathbf{G}_n(K)$ и $\mathbf{G}_m(M)$ ($\mathbf{G} = \mathrm{GL}, \mathrm{SL}, \mathrm{PGL}, \mathrm{PSL}$; K, M — поля характеристики 0) элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K и M элементарно эквивалентны. Дальнейшие исследования в этой области начались в 1992 г., когда

К. И. Бейдар и А. В. Михалёв [15] нашли единый подход к проблемам элементарной эквивалентности общих алгебраических структур и обобщили теорему Мальцева для случая, когда K и M являются телами и ассоциативными кольцами. Продолжением исследований в этой области стали работы Е. И. Буниной 1998—2010 гг. (см. [2—5]), 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.

Однако помимо того что можно рассматривать всё более разнообразные группы и обобщать теорему для случая элементарной эквивалентности, есть и иной путь, по которому может идти изучение вопроса, изначально поставленного Мальцевым, — это рассмотрение других видов эквивалентности. К примеру, можно обеднить теорию, разрешив использование только одного вида кванторов, а именно квантора всеобщности, и рассматривать алгебраические структуры в рамках этой обеднённой теории, называемой универсальной. Эквивалентность в рамках универсальных теорий называется *универсальной эквивалентностью*. 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]). Совсем недавно были получены результаты об универсальной эквивалентности линейных групп GL и специальных линейных групп SL над полями (Е. И. Бунина и Г. А. Калеева [6] и локальными коммутативными кольцами с 1/2 (Г. А. Калеева [9]).

Данная работа посвящена универсальной эквивалентности симплектических групп $\mathrm{Sp}_{2n}(K)$ над полями. В ходе доказательства используются критерий универсальной эквивалентности, сформулированный А. Д. Таймановым [12], и результаты из книги «Элементарная и близкие к ней логические эквивалентности классических и универсальных алгебр» Е. И. Буниной, А. В. Михалёва, А. Г. Пинуса [7]. Работа велась с помощью методов, схожих с теми, что были применены ранее для отыскания подобного критерия для линейных групп $\mathrm{GL}_n(K)$ и специальных линейных групп $\mathrm{SL}_n(K)$ Г. А. Калеевой [6]. Также много полезных технических деталей и приёмов было позаимствовано из работы М. Ф. Аль-Шедивата, Е. И. Буниной и А. В. Михалёва [1].

Авторы выражают признательность Галине Анатольевне Калеевой за многочисленные ценные советы и обсуждения задачи.

Целью данной работы является доказательство следующей теоремы.

Теорема 1 (критерий универсальной эквивалентности симплектических групп). *Пусть $n, m \geqslant 1$, K и M — бесконечные поля характеристики, отличной* *от 2. Тогда группы* $\mathrm{Sp}_{2n}(K)$ *и* $\mathrm{Sp}_{2m}(M)$ *универсально эквивалентны, если и только если*

1) $n = m$;
2) *поля* K *и* M *универсально эквивалентны.*

2. 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

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

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,

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

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) отображение f инъективно;
3) f сохраняет предикаты, функции и константы:
   а) для $P^n \in \Sigma$ и $a_0, \ldots, a_{n-1} \in \mathrm{dom}(f)$
   $$P_{\mathfrak{A}} a_0 \ldots a_{n-1} \Longleftrightarrow P_{\mathfrak{B}} f(a_0) \ldots f(a_{n-1});$$
   б) для $F^n \in \Sigma$ и $a_0, \ldots, a_{n-1}, a \in \mathrm{dom}(f)$
   $$F_{\mathfrak{A}}(a_0, \ldots, a_{n-1}) = a \Longleftrightarrow F_{\mathfrak{B}}\big(f(a_0), \ldots, f(a_{n-1})\big) = f(a);$$
   в) для $c \in \Sigma$ и $a \in \mathrm{dom}(f)$
   $$c_{\mathfrak{A}} = a \Longleftrightarrow c_{\mathfrak{B}} = f(a).$$

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

Определение 6. Симплектическая группа $\mathrm{Sp}_{2n}(K)$ — это группа матриц размера $2n \times 2n$ над полем K, удовлетворяющих условию

$$A^T Q A = Q,$$

где Q — фиксированная кососимметрическая матрица.

Замечание 1. В этой работе будем считать, что Q — это просто конкретная матрица вида

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

Важным свойством симплектической группы $\mathrm{Sp}_{2n}(K)$ является то, что это подгруппа $\mathrm{SL}_{2n}(K)$, а значит, все матрицы в ней имеют единичный определитель. Этим мы будем часто пользоваться.

Также в ходе доказательства будем пользоваться двумя важными соображениями.

Замечание 2. Так как отрицание универсальной формулы — экзистенциальная формула, то универсальная формула истинна в теории тогда и только тогда, когда экзистенциальная формула, являющаяся её отрицанием, ложна. А значит, вместо совпадения универсальных теорий можно доказывать совпадение экзистенциальных, что мы и будем делать, поскольку использование экзистенциальных формул удобнее для выделения конкретных элементов группы.

Теорема 2 (критерий универсальной эквивалентности [12]). *Пусть A и B — системы сигнатуры Σ. Для того чтобы системы A и B были универсально эквиваленты, необходимо и достаточно, чтобы для любой конечной подсигнатуры $\Sigma_1 \subset \Sigma$ любая конечная подсистема системы A сигнатуры Σ_1 была частично изоморфна некоторой подсистеме системы B той же сигнатуры, и наоборот.*

Замечание 3. Интересным является случай бесконечных полей K и M. Если поля K и M конечны, то универсальная эквивалентность совпадает с изоморфизмом и достаточно воспользоваться следующей теоремой (которая верна для целостных колец и тем более для полей) из лекций О'Миры о симплектических группах [11].

Теорема 3 (об изоморфизме симплектических групп [11]). *Пусть n, m — натуральные числа, $n, m > 2$, K, M — произвольные поля. Следующие утверждения равносильны*:

1) $n = m$ *и* $K \cong M$;
2) $\mathrm{Sp}_{2n}(K) \cong \mathrm{Sp}_{2m}(M)$.

Таким образом, далее будут рассматриваться лишь бесконечные поля характеристики, отличной от 2.

3. Доказательство в простую сторону и равенство размерностей

Предложение 1. *Пусть K и M — универсально эквивалентные бесконечные поля. Тогда для любого натурального m верно, что $\mathrm{Sp}_{2m}(K) \equiv_\forall \mathrm{Sp}_{2m}(M)$.*

Доказательство. Пусть $n = 2m$. Зададим симплектические группы как подсистемы в K^{n^2}:

$$\mathrm{Sp}_n(K) = \big\{(a_1 \dots a_{n^2}) \in K^{n^2} \mid A^T Q A = Q\big\},$$

где матричное умножение задаётся как перемножение элементов K^{n^2}, а именно по формуле

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

где

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

Матрице $A = (a_{ij})$, $i = 1, \dots, n$, $j = 1, \dots, n$, по правилу $a_{(i-1)n+j} = a_{ij}$ соответствует строка $(a_1, \dots, a_{n^2})$.

На базе этого любая конечная подсистема в $\mathrm{Sp}_n(K)$ задаётся как конечная подсистема в K^{n^2}, а поскольку поля универсально эквивалентны, для неё по теореме 2 можно найти конечную частично изоморфную ей подсистему в M^{n^2}. Следовательно, для исходной подсистемы в $\mathrm{Sp}_n(K)$ существует конечная частично изоморфная ей в $\mathrm{Sp}_n(M)$ и наоборот, а значит, $\mathrm{Sp}_{2m}(K) \equiv_\forall \mathrm{Sp}_{2m}(M)$. $\square$

Замечание 4. Предложение 1 также верно в случае, когда K и M являются коммутативными кольцами.

Снова предположим, что K и M — поля характеристики, отличной от?2, и выведем из универсальной эквивалентности $\mathrm{Sp}_{2n}(K)$ и $\mathrm{Sp}_{2m}(M)$ равенство размерностей $n = m$.

Лемма 1. *Максимальное число попарно коммутирующих инволюций в $\mathrm{Sp}_{2n}(K)$ равно в точности $2^n - 1$.*

Доказательство. Существует базис, в котором все попарно коммутирующие матрицы порядка 2 диагонализируемы. Тогда, поскольку для каждой матрицы $A \in \mathrm{Sp}_{2n}(K)$ справедливо $A^T Q A = Q$, их собственные значения могут быть лишь ± 1 и в этом базисе они имеют имеют вид $\mathrm{diag}[\pm\alpha_1, \pm\alpha_1, \dots, \pm\alpha_n, \pm\alpha_n]$, где $\alpha_i = \pm 1$. Таким образом, в $\mathrm{Sp}_{2n}(K)$ ровно $2^n - 1$ попарно коммутирующих матриц порядка 2. $\square$

Лемма 2. *Если $\mathrm{Sp}_{2n}(K) \equiv_\forall \mathrm{Sp}_{2m}(M)$ и бесконечные поля K и M имеют характеристику, отличную от 2, то $n = m$.*

Доказательство. Рассмотрим экзистенциальную формулу

$$\exists B_1, B_2, \ldots, B_N \left(\bigwedge_{i=1}^{N} \mathrm{Involution}(B_i) \mathbin{\&} \bigwedge_{\substack{i,j=1\\ i\neq j}}^{N} (\neg B_i = B_j) \mathbin{\&} \bigwedge_{i,j=1}^{N} (B_i B_j = B_j B_i) \right), \tag{1}$$

где

$$\mathrm{Involution}(X) := (X^2 = E) \wedge (X \neq E).$$

Так как группы универсально эквивалентны, то наибольшее N, такое что формула (1) истинна в обеих группах, одинаково для этих групп. $N = 2^n - 1 = 2^m - 1$ согласно предыдущей лемме, т. е. $n = m$. □

4. Дальнейшая схема доказательства

Идея состоит в том, чтобы выделить экзистенциальными формулами матрицу сложения и матрицу умножения, соответствующие некоторому элементу поля, а далее воспользоваться теоремой 2, а именно найти для произвольной конечной подмодели $K_1 \subset K$ конечную частично изоморфную ей подмодель $M_1 \subset M$, т. е. нужно построить частичный изоморфизм $\psi\colon K_1 \to M_1$.

Это будет сделано следующим образом: каждому элементу $\alpha \in K_1$ будут соответствовать некоторая матрица сложения, умножения и ещё несколько вспомогательных матриц. Назовём весь этот набор матриц $\mathfrak{A}(\alpha)$. Рассмотрим конечную подмодель $G_K \subset \mathrm{Sp}_{2n}(K)$, такую что $\mathfrak{A}(\alpha) \subset G_K$. Тогда согласно теореме 2 в $\mathrm{Sp}_{2n}(M)$ существует некоторая конечная подмодель G_M, частично изоморфная G_K, т. е. существует частичный изоморфизм $\phi\colon G_K \to G_M$. Нужно доказать, что частичный изоморфизм ϕ переводит все матрицы из $\mathfrak{A}(\alpha)$ в некоторую систему $\mathfrak{B}$ матриц того же вида, кроме того, образы матриц сложения и умножения должны соответствовать одному и тому же элементу β из поля M.

Искомая M_1 — множество всех элементов поля M, которые соответствуют парам образов матриц сложения и умножения для всех элементов из K_1. Для облегчения восприятия можно визуализировать идею доказательства следующей диаграммой:

$$\begin{tikzcd} \{\mathfrak{A}_\alpha\}_{\alpha\in K_1} \arrow[r, "\phi"] & \{\mathfrak{B}_\beta\}_{\beta\in M_1} \arrow[d] \\ K_1 \arrow[u] \arrow[r, "\psi"] & M_1 \end{tikzcd}.$$

После того как для $K_1 \subset K$ найдена частично изоморфная ей модель $M_1 \subset M$, воспользуемся опять теоремой 2, но уже в обратную сторону, и получим универсальную эквивалентность полей K и M в силу произвольности K_1.

5. Выделение необходимых матриц

5.1. Выделение инволюций

Замечание 5. С помощью формулы

$$\exists\, B_1, B_2, \dots, B_N \ \left(\bigwedge_{i=1}^{N} \mathrm{Involution}(B_i) \ \& \bigwedge_{\substack{i,j=1\\ i\neq j}}^{N} (\neg B_i = B_j) \ \& \bigwedge_{i,j=1}^{N} (B_iB_j = B_jB_i) \right),$$

где

$$\mathrm{Involution}(X) := (X^2 = E) \wedge (X \neq E),$$

можно выделить максимальный набор попарно коммутирующих инволюций, и все они одновременно в некотором базисе будут иметь диагональный вид

$$\mathrm{diag}[\pm\alpha_1, \pm\alpha_1, \dots, \pm\alpha_n],$$

где $\alpha_i = \pm 1$. Таким образом, в $\mathrm{Sp}_{2n}(K)$ ровно $2^n - 1$ попарно коммутирующих матриц порядка 2.

Замечание 6. Будем далее работать в выбранном базисе, где все вышеописанные инволюции диагональны.

Лемма 3 [1]. *В базисе, где некоторая матрица $A \in \mathrm{Sp}_{2n}(K)$ имеет вид*

$$\begin{pmatrix} E & 0 \\ 0 & -E \end{pmatrix},$$

форма Q принимает вид

$$\begin{pmatrix} Q_1 & 0 \\ 0 & Q_3 \end{pmatrix},$$

где Q_1 и Q_3 кососимметричны.

Замечание 7. Отсюда следует, что в базисе, где все попарно коммутирующие инволюции диагональны, форма Q имеет вид

$$Q = \begin{pmatrix} 0 & q_1 & \cdot & \cdot \\ -q_1 & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 0 & q_n \\ \cdot & \cdot & -q_n & 0 \end{pmatrix}, \quad q_i \in K^*, \quad i \in \{1, \dots, n\}.$$

Согласно замечанию 1 для матрицы Q выполнено $Q^2 = -E$. Следовательно, можно считать, что $q_i = \pm 1$. Причём на самом деле сейчас необязательно, чтобы знаки всех q_i в выбранном базисе совпадали, так как во всех формулах далее вплоть до раздела 5.8 мы будем использовать матрицу Q только в определении группы. А когда мы будем писать определение $AQA^T = Q$, нам будет неважно, какие знаки у q_i, поскольку мы будем иметь дело с блочно-диагональными матрицами. Таким образом, матрица Q не будет явно участвовать в экзистенциальных формулах вплоть до раздела 5.8, где она будет выделена.

5.2. Выделение блочно-диагональной матрицы с блоками из $\mathrm{SL}_2(K)$ на диагонали

Заметим, что если записать условие, что некоторая матрица A коммутирует со всем набором из попарно коммутирующих инволюций, которые мы выделили в предыдущем разделе, то получится, что такая матрица A имеет блочно-диагональный вид $\mathrm{diag}[\mathrm{SL}_2(K),\dots,\mathrm{SL}_2(K)]$ в том смысле, что в блоках 2×2 на диагонали могут стоять произвольные матрицы из $\mathrm{SL}_2(K)$, а в остальных местах — нули. Такое выделение осуществляется с помощью экзистенциальной формулы

$$\mathrm{Block}(A) := \exists\, B_1, B_2, \dots, B_N\ \Bigl(\bigwedge_{i=1}^{N}(B_iA = AB_i)\Bigr). \tag{2}$$

Набор $B_1, B_2, \dots, B_N$ выделен формулой (1).

5.3. Выделение частичной трансвекции

Лемма 4. *Блочно-диагональная матрица частичной трансвекции, т. е. такая матрица, что в некотором базисе у неё хотя бы в одном из блоков 2×2 на главной диагонали стоит матрица*

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

а значит, с точностью до перестановки блоков она имеет вид

$$\begin{pmatrix}T & \cdot & \cdot & \cdot\\ \cdot & M_2 & \cdot & \cdot\\ \cdot & \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot & M_n,\end{pmatrix}$$

где

$$T = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\quad M_i \in \left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}\alpha & 0\\ 0 & 1/\alpha\end{pmatrix}\right\},$$

выделяется экзистенциальной формулой.

Доказательство. Рассмотрим матрицу A, удовлетворяющую формуле

$$\mathrm{PTransvection}(A) := \exists\, X\bigl(\mathrm{Block}(A)\ \&\ \mathrm{Block}(X)\ \&\ (X^2A^2 \neq A^2X^2)\ \&\\ \&\ (XAX^{-1}A = AXAX^{-1})\ \&\ (XAX^{-1} = A^4)\bigr). \tag{3}$$

Заметим, что для матрицы A с блоками

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

на диагонали эта формула истинна, например, при X с блоками

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

на диагонали. Поскольку $\mathrm{char}(K) \neq 2$, то $2, 1/2 \in K$, и такая X есть в нашей группе $\mathrm{Sp}_{2n}(K)$.

Все матрицы, удовлетворяющие формуле

$$\exists\, A \;\; \mathrm{PTransvection}(A),$$

блочно-диагональны и имеют вид

$$A = \mathrm{diag}[A_1, \ldots, A_n], \quad X = \mathrm{diag}[X_1, \ldots, X_n],$$

где все A_i и X_i лежат в $\mathrm{SL}_2(K)$.

Разобьём формулу 3 на две части, без отрицания и с отрицанием:

$$\begin{aligned} &\phi(A, X) = (XAX^{-1}A = AXAX^{-1})\, \&\, (XAX^{-1} = A^4),\\ &\psi(A, X) = (X^2A^2 \neq A^2X^2). \end{aligned}$$

Заметим, что формула

$$\exists\, A \;\; \mathrm{PTransvection}(A)$$

является истинной тогда и только тогда, когда условие $\phi(A_i, X_i)$ выполняется для всех пар A_i и X_i, а условие $\psi(A_i, X_i)$ выполняется хотя бы для одной пары A_i и X_i.

Пусть теперь для некоторой матрицы $A' \in \mathrm{SL}_2(K)$ истинна формула

$$\exists\, X \;\; \phi(A', X) \wedge \psi(A', X).$$

Если жорданова форма матрицы A' над $\bar{K}$ не диагональна, то она равна

$$A_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

или

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

Второй случай не реализуется, так как

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

а это значит, что A_-^4 не сопряжена с A_-, поскольку у одной из них собственное значение -1, а у другой 1.

Если матрица A' диагонализируема над $\bar{K}$, то её диагональная форма имеет вид $\mathrm{diag}[\alpha, 1/\alpha]$, причём $\alpha \neq \pm 1$, поскольку $(A')^2 \neq E$ (что следует из истинности $\psi(A, X)$). Пусть

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

произвольная матрица. Тогда из соотношения $XA'X^{-1}A' = A'XA'X^{-1}$ получаем

$$\begin{pmatrix} ad\alpha^2 - bc & -ab + ab/\alpha^2 \\ cd\alpha^2 - cd & -bc + ad/\alpha^2 \end{pmatrix} = \begin{pmatrix} ad\alpha^2 - bc & ab - ab\alpha^2 \\ -cd/\alpha^2 + cd & -bc + ad/\alpha^2 \end{pmatrix},$$

а из соотношения $X^2A'^2 \neq A'^2X^2$ получаем

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

Из первого условия мы получаем $cd(2-\alpha^2-1/\alpha^2)=0$ и $ab(2-\alpha^2-1/\alpha^2)=0$, а значит, $ab=cd=0$, поскольку $\alpha \neq \pm 1$.

Имеем, что $ad-bc=1$, а значит, a и c не могут одновременно равняться нулю, следовательно, если $a=0$, то и $d=0$. Аналогично если $b=0$, то $c=0$. Поэтому $ab+bd=ac+cd=0$, что противоречит формуле $X^2A' \neq A'X^2$. Значит, жорданова форма A' над $\bar{K}$ не диагональна, т. е. имеет вид

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

и матрица A, которая выделяется формулой $\mathrm{PTransvection}(A)$, имеет в некотором базисе блочно-диагональный вид с хотя бы одним блоком

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

на диагонали. Заметим также, что остальные блоки матрицы A либо имеют такую же жорданову форму, либо диагонализируемы. Таким образом, выделена искомая матрица A. □

5.4. Выделение матрицы $-E$

Лемма 5. *Матрица $-E$ выделяется экзистенциальной формулой*

Доказательство. Разобьём инволюции $B_1,\dots,B_N$, полученные в разделе 5.1, на классы сопряжённости. Ясно, что в один класс могут попасть лишь матрицы с одинаковым количеством пар из -1 на главной диагонали. Поскольку мы знаем размерность n группы $\mathrm{Sp}_{2n}(K)$, то мы знаем, что самый большой класс сопряжённости содержит $C_n^{[n/2]}$ элементов — это инволюции с $[n/2]$ или $n-[n/2]$ парами из -1 на главной диагонали. Таких классов один или два в зависимости от чётности n. А значит, записав конъюнкцию условий, что все матрицы внутри класса сопряжены (или сопряжены с первой), они являются попарно коммутирующими инволюциями и их ровно $C_n^{[n/2]}$, мы выделим нужный класс:

$$\exists B_1,B_2,\dots,B_{[n/2]}\ \exists C_2,\dots,C_{[n/2]}\ \Bigg(\bigwedge_{i=1}^{[n/2]}\mathrm{Involution}(B_i)\ \&\ \bigwedge_{\substack{i,j=1\\ i\neq j}}^{[n/2]}(\neg B_i=B_j)\ \& \\ \&\ \bigwedge_{i,j=1}^{[n/2]}(B_iB_j=B_jB_i)\ \&\ \bigwedge_{i=2}^{[n/2]}(B_1C_i=C_iB_i)\Bigg).$$

Если же классов два, то запишем такую же формулу и добавим условие, что какая-нибудь матрица из нового класса не равна никакой матрице из уже выделенного, это обеспечит выделение другого, а не того же самого класса:

$$\exists\, B'_1, B'_2, \ldots, B'_{[n/2]}\ \exists\, C_2, \ldots, C_{[n/2]} \Biggl(\bigwedge_{i=1}^{[n/2]} \mathrm{Involution}(B'_i)\ \&\ \bigwedge_{\substack{i,j=1\\ i\neq j}}^{[n/2]} (\neg B'_i = B'_j)\ \&$$
$$\&\ \bigwedge_{i,j=1}^{[n/2]} (B'_i B'_j = B'_j B'_i)\ \&\ \bigwedge_{i=2}^{[n/2]} (B'_1 C_i = C_i B'_i)\ \&\ \bigwedge_{j=1}^{[n/2]} (\neg B'_1 = B_j) \Biggr).$$

Далее продолжим эту процедуру. Будем выделять по очереди классы с $[n/2]-k$ и $n-[n/2]+k$ пар из -1 на главной диагонали для всех $k = 1, \ldots, [n/2]$. Для каждого нового класса будем писать, что какая-то матрица в нём не равна ни одной из уже выделенных. Это будет обеспечивать нам выделение действительно новых классов каждый раз. В конце у нас останутся только два одноэлементных класса: матрица E и матрица $-E$, т. е. $-E$ выделится как инволюция из набора, полученного в 5.1, не равная ни одной из выделенных в вышеописанном процессе матриц и отличная от E. □

5.5. Выделение инволюций B_i с одной парой -1 на диагонали, а также матриц X_i

Из множества диагональных инволюций в $\mathrm{Sp}_{2n}(K)$, выделенных в разделе 5.1, выделим те, у которых ровно одна пара -1 на главной диагонали.

Наложим два условия: они все лежат в одном классе сопряжённости, количество элементов в этом классе равно n. Ясно, что таким условиям удовлетворяют ровно два класса инволюций: те, у которых одна пара -1 на главной диагонали, и те, у которых $n-1$ таких пар.

Замечание 8. Ясно, что при $n=2$ указанные классы совпадают, а при $n \geqslant 3$ проходит следующее доказательство.

Запишем условие, которое поможет нам различить эти классы.

Пусть
$$B_1 = \mathrm{diag}\left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right].$$

Замечание 9. Если $X_1^2 = B_1$, то в некотором базисе
$$X_1 = \left[\mathrm{diag}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \ldots, \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}\right].$$

Доказательство. Рассмотрим левый верхний блок матрицы X_1. Пусть его жорданова форма над $\bar{K}$ равна
$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Но тогда
$$\begin{pmatrix}\lambda^2 & 2\lambda\\ 0 & \lambda^2\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$
Отсюда следует, что $\lambda^2 = -1$, но $\lambda^2 = 1$, поскольку определитель этого блока равен 1. Таким образом, получили противоречие. Следовательно, матрица X_1 диагонализируема над $\bar{K}$ и с точностью до замены базиса равна
$$\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}.$$
Но эта матрица сопряжена с матрицей
$$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},$$
которая лежит в $\mathrm{SL}_2(K)$. □

Заметим теперь, что если некоторая матрица C коммутирует с X_1, то C в этом базисе имеет вид
$$\mathrm{diag}\left[\begin{pmatrix}a & c\\ -c & a\end{pmatrix}, \mathrm{SL}_2(K), \ldots, \mathrm{SL}_2(K)\right].$$
Заметим, что матрицы
$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$
и
$$\begin{pmatrix}a & c\\ -c & a\end{pmatrix}$$
имеют разные жордановы формы, а значит, ни в каком базисе не совпадают.

Пусть B_i — инволюция с одной парой -1 на диагонали, такая что эти -1 стоят в i-м блоке. Тогда если мы запишем формулу $X_1C = CX_1 \wedge X_2C = CX_2$ и ещё наложим условие $\mathrm{PTransvection}(C)$, то с помощью этой формулы у нас выделится какая-то матрица, поскольку после наложения первого условия в общем виде матрицы C останется хоть один блок $\mathrm{SL}_2(K)$ на главной диагонали. Если же изначально выделенные инволюции были с $n-1$ парой -1 на главной диагонали, то матрица C после наложения условия $X_1C = CX_1 \wedge X_2C = CX_2$ должна иметь лишь блоки вида
$$\begin{pmatrix}a & c\\ -c & a\end{pmatrix}$$
на главной диагонали, а значит, после наложения условия $\mathrm{Transvection}(C)$ никакая матрица не выделится. Ясно, что все действия, описанные в этом разделе, записываются экзистенциальной формулой, а значит, так мы можем различить инволюции с одной и $n-1$ парами -1 на главной диагонали.

Таким образом, мы научились выделять матрицы инволюций B_i с одной парой -1 на главной диагонали и матрицы X_i, которые имеют вид

$$\mathrm{diag}\left[\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix},\ldots,\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ldots,\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix}\right],$$

где блок

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

стоит на i-м месте.

5.6. Выделение матриц перестановки блоков

Определение 7. Матрица S_{ij} перестановки блоков — это такая матрица, при сопряжении которой меняются местами i-й и j-й блоки в блочно-диагональной матрице. Она имеет вид

$$S_{ij} = \pm\begin{pmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}$$

(тут для простоты опущены все остальные (2×2)-блоки, которые расположены на главной диагонали матрицы S_{ij} и имеют вид

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

все остальные элементы нулевые).

Лемма 6. *Матрицы перестановки блоков выделяются экзистенциальной формулой.*

Доказательство. Матрицы перестановки блоков S_{ij} характеризуются следующими условиями:

1) S_{ij} коммутируют со всеми инволюциями B_k при $k \neq i, j$;
2) $S_{ij}B_iS_{ij}^{-1} = B_j$, где B_i — выделенная в разделе 5.5 инволюция с одной парой -1 в i-м блоке на главной диагонали;
3) S_{ij} сохраняет форму Q;
4) $S_{ij}X_i = X_jS_{ij}$ и $S_{ij}X_j = X_iS_{ij}$, где X_i — выделенная в разделе 5.5 матрица

$$\mathrm{diag}\left[\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix},\ldots,\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ldots,\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix}\right]$$

с

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

в i-м блоке на главной диагонали;

5) $S_{ij}^2 = E$;

6) $S_{ij}\pi S_{ij} = \pi$, где π — матрица частичной трансвекции, у которой блок

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

стоит на i-м месте на главной диагонали.

Рассмотрим сперва блок матрицы S_{ij} размером 4×4, образованный из элементов, находящихся на пересечении $(2i-1)$-го, $(2i)$-го, $(2j-1)$-го и $(2j)$-го столбцов с $(2i-1)$-й, $(2i)$-й, $(2j-1)$-й и $(2j)$-й строками матрицы S_{ij}. Обозначим этот блок через S.

После применения условий 1) и 2) получаем, что данный блок имеет вид

$$\begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & c & d\\ e & f & 0 & 0\\ g & h & 0 & 0\end{pmatrix}.$$

По условию 3) имеем

$$\begin{pmatrix}0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{pmatrix} = \begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & c & d\\ e & f & 0 & 0\\ g & h & 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{pmatrix}\begin{pmatrix}0 & 0 & e & g\\ 0 & 0 & f & h\\ a & c & 0 & 0\\ b & d & 0 & 0\end{pmatrix} =$$

$$= \begin{pmatrix}0 & ad-bc & 0 & 0\\ bc-ad & 0 & 0 & 0\\ 0 & 0 & 0 & eh-gf\\ 0 & 0 & gf-eh & 0\end{pmatrix}.$$

Отсюда следует, что $ad-bc = eh-gf = 1$.

По первой части условия 4) имеем

$$\begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & c & d\\ e & f & 0 & 0\\ g & h & 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{pmatrix}\begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & c & d\\ e & f & 0 & 0\\ g & h & 0 & 0\end{pmatrix},$$

т. е.

$$\begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & c & d\\ f & -e & 0 & 0\\ h & -g & 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & c & d\\ -g & -h & 0 & 0\\ e & f & 0 & 0\end{pmatrix}.$$

Отсюда следует, что $h=e$, $g=-f$; аналогично из второй части условия 4) получаем $a=d$ и $b=-c$. После наложения этих условий можно считать, что

$$S = \begin{pmatrix}0 & 0 & a & b\\ 0 & 0 & -b & a\\ e & f & 0 & 0\\ -f & e & 0 & 0\end{pmatrix}.$$

По условию 5) имеем

$$S^2 = \begin{pmatrix} ae-bf & af+be & 0 & 0 \\ -(af+be) & ae-bf & 0 & 0 \\ 0 & 0 & ae-bf & af+be \\ 0 & 0 & -(af+be) & ae-bf \end{pmatrix} = E,$$

т. е. из условий 3) и 5) получаем систему

$$\begin{cases} ae-bf=1, \\ af=-be, \\ a^2+b^2=1, \\ e^2+f^2=1. \end{cases}$$

Возможны два случая.

— $e=0$. Тогда получаем $bf=-1$ и $af=0$, а значит, $a=0$. Имеем $b^2 = f^2 = 1$, откуда с учётом $bf=-1$ получаем, что $f=\pm 1$ и $b=\pm f$, т. е.

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

— $e \neq 0$. Подставим $b=-af/e$ в $ae-bf=1$ и домножим эту строчку на e. Получим $a(e^2+f^2)=e$, откуда с учётом $(e^2+f^2)=1$ следует, что $a=e$. Подставим $a=e$ в $af=-be$, откуда с учётом $e\neq 0$ получим, что $f=-b$. С учётом этих равенств имеем

$$S = \begin{pmatrix} 0 & 0 & a & b \\ 0 & 0 & -b & a \\ a & -b & 0 & 0 \\ b & a & 0 & 0 \end{pmatrix}.$$

Отвлечёмся теперь от блока S и поймём, что произошло после наложения условий 1)—5) с остальной частью матрицы S_{ij}. Условие 1) занулило все элементы матрицы S_{ij}, кроме блоков размера 2×2 на главной диагонали и блока S. Рассмотрим произвольный такой блок, пусть он имеет вид

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

Условие 3) обеспечивает, что $ad-bc=1$. Запишем теперь условие 5) для произвольного такого блока, получим

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

Рассмотрим два возможных случая.

— $a + d \neq 0$. Тогда получаем $b = c = 0$ и $a^2 = d^2 = ad = 1$, а значит, $a = d = \pm 1$.

— $a + d = 0$. Подставим $a = -d$ в $ad - bc = 1$, с учётом $a^2 + bc = 1$ получим несовместную систему

$$\begin{cases} -a^2 - bc = 1, \\ a^2 + bc = 1. \end{cases}$$

Следовательно, рассматриваемый блок имеет вид

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

Рассмотрим теперь условие 6). Пусть в нашем базисе матрица частичной трансвекции π имеет вид

$$\mathrm{diag}[M_1, \ldots, T, \ldots, M_n],$$

где

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad M_k \in \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \right\},$$

а блок T стоит на i-м месте.

Обозначим через Tr блок размером 4×4, образованный из элементов, находящихся на пересечении $(2i-1)$-го, $(2i)$-го, $(2j-1)$-го и $(2j)$-го столбцов с $(2i-1)$-й, $(2i)$-й, $(2j-1)$-й и $(2j)$-й строками матрицы π. Есть два случая:

$$\mathrm{Tr} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \frac{1}{\alpha} \end{pmatrix} \quad \text{и} \quad \mathrm{Tr} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда с учётом $S_{ij} \pi S_{ij} = \pi$ для Tr и S в первом случае имеем

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

Следовательно,

$$\begin{pmatrix} \alpha a^2 + (1/\alpha) b^2 & ab(1/\alpha - \alpha) & 0 & 0 \\ ab(1/\alpha - \alpha) & (1/\alpha) a^2 + \alpha b^2 & 0 & 0 \\ 0 & 0 & 1 - ab & a^2 \\ 0 & 0 & -b^2 & 1 + ab \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 1/\alpha \end{pmatrix}.$$

Отсюда получаем, что $a = b = 0$, а значит, первый случай несовместен, поскольку не выполняется условие $a^2 + b^2 = 1$.

Во втором случае имеем

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

т. е.

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

Отсюда следует, что $b = 0$ и $a = \pm 1$, а значит, в итоге получаем, что

$$S = \pm\begin{pmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}.$$

Таким образом, матрицы перестановок блоков S_{ij} выделяются экзистенциальными формулами, которые получаются конъюнкцией условий 1), 2), 4), 5) и 6). Заметим, что все матрицы, встречающиеся в этих условиях, выделяются экзистенциальными формулами. Условие 3) можно не включать в формулу, поскольку оно и так верно для всех матриц из $\mathrm{Sp}_{2n}(K)$. Поэтому неважно, что мы ещё не научились выделять матрицу Q. □

5.7. Выделение трансвекции

Определение 8. Матрица трансвекции — это блочно-диагональная матрица, имеющая вид

$$\begin{pmatrix}T & 0 & \cdot & 0\\ 0 & T & \cdot & 0\\ \cdot & \cdot & \cdot & \cdot\\ 0 & 0 & \cdot & T\end{pmatrix},$$

где

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

Лемма 7. *Матрица трансвекции выделяется экзистенциальной формулой.*

Доказательство. Рассмотрим матрицу A, удовлетворяющую формуле

$$\mathrm{Transvection}(A) := \left(\mathrm{PTransvection}(A)\ \&\ \left(\bigwedge_{i=1}^{n}(S_{1i}A = AS_{1i})\right)\right). \qquad (4)$$

Матрица A является частичной трансвекцией, т. е. с точностью до перестановки блоков размера 2×2 на главной диагонали она имеет вид

$$\begin{pmatrix} T & 0 & \cdot & 0 \\ 0 & M_2 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & M_n \end{pmatrix},$$

где

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad M_i \in \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{pmatrix} \right\}.$$

Кроме того, у неё все блоки размера 2×2 на главной диагонали одинаковые, а значит, это в точности матрица трансвекции. $\square$

5.8. Выделение матрицы Q

Матрица Q — это блочно-диагональная матрица с блоками

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

на диагонали.

Лемма 8. *Матрица Q выделяется формулой*

$$\exists Q\ \exists \sigma\ \big(\mathrm{Block}(Q)\ \&\ \mathrm{Transvection}(\sigma)\ \&\ (Q^2 = -E)\ \&\ (Q\sigma Q = -\sigma^{-1} Q \sigma^{-1})\big).$$

Доказательство. Напомним, что мы работаем в базисе, где σ имеет блочно-диагональный вид с блоками

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

на диагонали. Рассмотрим один из блоков матрицы Q — для определённости, например, левый верхний. Пусть он имеет произвольный вид

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

Тогда из $Q^2 = -E$ получим для выбранного блока

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

Из условия $Q\sigma Q = -\sigma^{-1} Q \sigma^{-1}$ получим

$$\begin{pmatrix} a^2 + (a+b)c & ab + (a+b)d \\ c(a+c+d) & bc + d(c+d) \end{pmatrix} = \begin{pmatrix} -a + c & a - b - c + d \\ -c & c - d \end{pmatrix}.$$

Заметим, что $b(a + d) = c(a + d) = 0$. Пусть $a + d \neq 0$. Тогда $b = c = 0$, следовательно, $a^2 = -a$ и $a^2 = -1$. Этот случай несовместен, значит, $a + d = 0$ и тогда $a^2 + bc = -1$. Кроме того, $c^2 = -c$, а значит, $c = -1$, поскольку выше показано, что $c \neq 0$. Тогда $b = a^2 + 1$. Таким образом, выбранный блок имеет вид

$$\begin{pmatrix} a & 1 + a^2 \\ -1 & a \end{pmatrix}.$$

Проведём замену базиса с помощью матрицы, у которой в соответствующем блоке стоит

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

а на остальных местах на диагонали единицы, и получим нужный нам вид выбранного блока матрицы Q. Заметим, что такая замена базиса не повлияет на матрицу σ, поскольку она коммутирует с матрицей перехода. Понятно, что аналогично получается нужный вид всех остальных блоков. □

5.9. Выделение диагональных матриц

Лемма 9. *Диагональная матрица D выделяется экзистенциальной формулой*

$$\mathrm{Diag}(D) := \exists\, D\ \exists\, \sigma\ \big(\mathrm{Block}(D)\ \&\ \mathrm{Transvection}(\sigma)\ \&$$
$$\&\ (QDQ^{-1} = D^{-1})\ \&\ (D\sigma D^{-1}\sigma = \sigma D\sigma D^{-1})\big),$$

где матрица Q — матрица, полученная в разделе 5.8.

Доказательство. Рассмотрим, как и в предыдущих леммах, левый верхний блок матрицы D. Пусть он имеет произвольный вид

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

Тогда из $QDQ^{-1} = D^{-1}$ получим

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

т. е. $b = c$. Из $D\sigma D^{-1}\sigma = \sigma D\sigma D^{-1}$ получим

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

т. е. $b^2 = 0$, а значит, $b = 0$.

Таким образом, выбранный блок имеет вид

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Но поскольку этот блок есть матрица из $\mathrm{SL}_2(K)$, то $d = 1/a$, а значит, выбранный блок имеет вид

$$\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}.$$ □

Определение 9. Матрицу $\mathrm{Pr}(a)$, состоящую из блоков

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

на главной диагонали, назовём *матрицей умножения, соответствующей элементу a.*

Замечание 10. Заметим, что пока что мы выделили лишь диагональную матрицу, в которой в разных блоках размера 2×2 могут стоять разные элементы, а значит, она ещё не является матрицей умножения.

5.10. Выделение матриц умножения

Матрицы умножения — это в точности диагональные матрицы D с условием, что $SDS^{-1} = D$, которое верно при всевозможных матрицах перестановок блоков S. Это условие обеспечивает совпадение элементов во всех блоках диагональной матрицы D, а значит, после его применения она имеет вид

$$D = \operatorname{diag}\left[\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \ldots, \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}\right].$$

Замечание 11. Описанное выше условие записывается экзистенциальной формулой путём перечисления всех матриц перестановок блоков, поскольку их конечное число. А значит, матрица умножения выделяется экзистенциальной формулой $\mathrm{ProductMatrix}$.

5.11. Матрица сложения

Определение 10. Матрицу $\mathrm{Sum}(a)$, состоящую из блоков

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

на главной диагонали, назовём *матрицей сложения, соответствующей элементу* a.

Матрицы сложения — это матрицы, которые коммутируют с трансвекциями.

Лемма 10. *Матрицы сложения* Sum *выделяется экзистенциальной формулой.*

Доказательство. Рассмотрим формулу

$$\begin{aligned} &\mathrm{SumMatrix}(A) := \\ &\quad := \exists\, A\ \exists\, \sigma\ \exists\, D\ \bigl(\mathrm{Block}(A)\ \&\ \mathrm{Transvection}(\sigma)\ \&\ \mathrm{ProductMatrix}(D)\ \& \\ &\quad \&\ (A\sigma = \sigma A)\ \&\ (DAD^{-1} = A^4)\bigr). \end{aligned}$$

Кроме того, наложим условие, что матрица A коммутирует со всеми матрицами перестановок блоков, выделенными в разделе 5.6. Это обеспечит нам одинаковые блоки размера 2×2 на главной диагонали матрицы A. Рассмотрим левый верхний блок матрицы A. Пусть он имеет вид

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

После наложения условия $A\sigma = \sigma A$ получаем, что этот блок имеет вид

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix},$$

причём с учётом того, что данная матрица принадлежит $\mathrm{SL}_2(K)$, имеем $a = \pm 1$. Пусть D — матрица умножения, соответствующая элементу α. Тогда после наложения условия $DAD^{-1} = A^4$ имеем

$$\begin{pmatrix} \pm 1 & \alpha^2 b \\ 0 & \pm 1 \end{pmatrix} = \begin{pmatrix} 1 & 4b \\ 0 & 1 \end{pmatrix}.$$

Таким образом, получаем, что $a = 1$ и матрица A имеет вид

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}. \qquad \square$$

6. Заключение

6.1. Связь матриц сложения и умножения

Заметим, что блоки размера 2×2 в матрицах сложения и умножения, соответствующих одному и тому же элементу x, связаны формулой

$$\begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} = -\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1/x & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{5}$$

Заметим, что

$$\begin{pmatrix} 1 & 0 \\ -1/x & 1 \end{pmatrix} = Q \operatorname{Sum}(x^{-1}) Q^{-1},$$

а значит, формула (5) переписывается как

$$\operatorname{Pr}(x) = -\operatorname{Sum}(x) Q \operatorname{Sum}(x^{-1}) Q^{-1} \operatorname{Sum}(x) Q. \tag{6}$$

Таким образом, если при частичном изоморфизме $\Phi\colon \mathrm{Sp}_{2n}(K) \to \mathrm{Sp}_{2n}(M)$ сохраняется вид матриц сложения, матриц умножения и всех вспомогательных матриц и матрица сложения и умножения соответствует одному и тому же элементу в поле K, то их образы при изоморфизме Φ также будут соответствовать одному и тому же элементу поля M.

6.2. Завершение доказательства

Осталось показать, что при частичном изоморфизме выделенные в разделе 5 матрицы сохраняют вид.

Матрицы умножения, матрицы сложения, а также вспомогательные матрицы выделены экзистенциальными формулами в группе $\mathrm{Sp}_{2n}(K)$. Поскольку $\mathrm{Sp}_{2n}(K) \equiv_\forall \mathrm{Sp}_{2n}(M)$, то эти же формулы верны и для образов матриц, полученных при частичном изоморфизме. Значит, все необходимые матрицы сохраняют вид при частичном изоморфизме, поскольку такой изоморфизм сохраняет формулы. Далее остаётся воспользоваться теоремой 2, действуя в точности как указано в разделе 4. Таким образом, из универсальной эквивалентности групп $\mathrm{Sp}_{2n}(K)$ и $\mathrm{Sp}_{2m}(M)$ следует универсальная эквивалентность полей K и M, что с учётом равенства $n = m$, полученного в лемме 2, завершает доказательство теоремы 1.

Литература

[1] Аль-Шедиват М. Ф., Бунина Е. И., Михалёв А. В. Элементарная определимость линейных классических и симплектических групп над полями // Фундамент. и прикл. матем. — В печати.

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

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

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

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

[6] Бунина Е. И., Калеева Г. А. Универсальная эквивалентность общих и специальных линейных групп над полями // Фундамент. и прикл. матем. — 2016. — Т. 21, вып. 3. — С. 73—106.

[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] Калеева Г. А. Универсальная эквивалентность линейных групп над локальными коммутативными кольцами с 1/2 // Алгебра и логика. — 2019. — Т. 58, № 4. — С. 467—478.

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

[11] О'Мира О. Лекции о симплектических группах. — М.: Мир, 1979.

[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 Malcev's theorem on elementary equivalence of linear groups // Contemp. Math. — 1992. — 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.