Элементарная эквивалентность стабильных линейных групп над полями характеристики два*

Е. И. БУНИНА
Университет им. Бар-Илана, Израиль
e-mail: helenbunina@gmail.com

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

И. О. СОЛОВЬЁВ
Московский государственный университет им. М. В. Ломоносова
e-mail: hayer44@yandex.ru

УДК 510.67+512.54

Ключевые слова: стабильные линейные группы, элементарная эквивалентность, поля характеристики 2.

Аннотация

В данной работе мы доказываем критерий элементарной эквивалентности стабильных линейных групп над полями характеристики 2.

Abstract

E. I. Bunina, A. V. Mikhalev, I. O. Solovyev, Elementary equivalence of stable linear groups over fields of characteristic 2, Fundamentalnaya i prikladnaya matematika, vol. 24 (2023), no. 3, pp. 11—21.

In this paper, we prove a criterion of elementary equivalence of stable linear groups over fields of characteristic 2.

1. Введение: история и определения

1.1. Элементарная эквивалентность

Две структуры одинаковой сигнатуры называются *элементарно эквивалентными*, если в них выполняются одинаковые предложение на языке первого порядка в их сигнатуре. Любые две конечные структуры элементарно эквивалентны тогда и только тогда, когда они изоморфны. Любые две изоморфные структуры элементарно эквивалентны, но обратное не обязательно верно. Например, поле комплексных чисел $\mathbb{C}$ и поле алгебраических чисел $\bar{\mathbb{Q}}$ элементарно эквивалентны, но не могут быть изоморфными, так как имеют разную мощность.

*Работа второго автора финансово поддержана Российским научным фондом, грант 22-11-00052.

А. Тарскому и А. И. Мальцеву принадлежат первые результаты, связанные с описанием групп и колец с точки зрения элементарной эквивалентности. Было получено несколько полных результатов классификации алгебраических структур с точностью до элементарной эквивалентности: например, два алгебраически замкнутых поля элементарно эквивалентны тогда и только тогда, когда они имеют одинаковую характеристику; две абелевы группы элементарно эквивалентны тогда и только тогда, когда у них одинаковы специальные характеристические числа (В. Шмелев, см. [27]). Похожие результаты были получены для булевых колец (Ю. Л. Ершов и А. Тарский, см. [14]).

Выдающимся достижением было решение старых проблем, поднятых А. Тарским в 1945 году: свободные группы не могут быть отличимы при помощи элементарной теории (см. результаты серии работ О. Харлампович и А. Мясникова и Ц. Селы, в том числе [22, 23]). Похожая ситуация возникает со свободными гиперболическими группами без кручения (Ц. Села, см. [24]).

1.2. Теоремы мальцевского типа для линейных групп

Другая интересная сфера для изучения — это связь между логическими свойствами каких-то базовых структур и логическими свойствами их производных структур.

Первые результаты такого типа были получены А. И. Мальцевым в [16]. Он доказал, что группы $\mathcal{G}_n(K_1)$ и $\mathcal{G}_m(K_2)$ (где $G = \mathrm{GL}, \mathrm{SL}, \mathrm{PGL}, \mathrm{PSL}$, $n, m \geqslant 3$, K_1, K_2 — поля характеристики 0) элементарно эквивалентны тогда и только тогда, когда $m = n$ и поля K_1 и K_2 элементарно эквивалентны. Такое соответствие часто называют *мальцевским соответствием* или *мальцевским переносом*. Это свойство означает, что все логические свойства полностью переносятся с базовых структур на производные и наоборот.

В 1961—1971 годах Г. Кейслер (см. [21]) и С. Шелах (см. [25]) доказали важную теорему об изоморфизме.

Теорема 1. *Две модели $\mathcal{U}_1$ и $\mathcal{U}_2$ элементарно эквивалентны тогда и только тогда, когда существует ультрафильтр $\mathcal{F}$, такой что соответствующие ультрастепени изоморфны*:

$$\prod_{\mathcal{F}} \mathcal{U}_1 \cong \prod_{\mathcal{F}} \mathcal{U}_2.$$

Эта теорема позволила К. И. Бейдару и А. В. Михалёву в 1992 году (см. [17]) обобщить теорему Мальцева для случая, когда K_1 и K_2 — тела или первичные ассоциативные кольца. Этот подход для групп GL_n был обобщён в [2], где был получен следующий результат.

Теорема 2. *Пусть R_1 и R_2 — это ассоциативные кольца с* 1 (1/2) *с конечным числом центральных идемпотентов $m, n \geqslant 4$ ($m, n \geqslant 3$). Тогда $\mathrm{GL}_m(R_1) \equiv \mathrm{GL}_n(R_2)$ тогда и только тогда, когда существуют центральные идемпотенты $e \in R$ и $f \in S$, такие что $eM_m(R) \equiv fM_n(S)$ и $(1-e)M_m(R) \equiv (1-f)M_n(S)^{\mathrm{op}}$.*

Исследование было продолжено в работах Е. И. Буниной в 1998—2010 годах. Результаты, схожие с теоремой Мальцева, были получены не только для классических групп GL, PGL, SL, PSL, но также для унитарных линейных групп над полями, телами и кольцами с инволюциями (см. [3, 4]), для групп Шевалле над полями (см. [5]), локальными кольцами (см. [6]), произвольными коммутативными кольцами (см. [7]) и также для других различных производных структур.

В некоторых случаях элементарная эквивалентность производных структур (даже сколько-то близких к линейным группам) равносильна не элементарной эквивалентности исходных структур, а их более сильной логической эквивалентности. Часто требуется эквивалентность в логике второго порядка или какие-то её ограничения.

Например, в 2000 г. В. Толстых [28] установил связь между свойствами второго порядка тел и свойствами первого порядка групп автоморфизмов бесконечномерных линейных пространств над ними. В 2003 г. Е. И. Бунина и А. В. Михалёв (см. [9]) показали связь между свойствами второго порядка ассоциативных колец и элементарными свойствами категорий модулей, колец эндоморфизмов, групп автоморфизмов и проективных пространств бесконечного ранга над этими кольцами. Похожие результаты получались и для колец эндоморфизмов и групп автоморфизмов абелевых p-групп: Е. И. Бунина, А. В. Михалёв и М. А. Ройзнер (см. [11]) доказали, что два кольца эндоморфизмов абелевых p-групп или две группы автоморфизмов абелевых p-групп при $p \geqslant 3$ элементарно эквивалентны тогда и только тогда, когда исходные абелевы групп эквивалентны в полной логике второго порядка (в одном исключительном случае — в её ограничении).

1.3. Стабильные линейные группы

Пусть R — ассоциативное кольцо с единицей. Следующие определения соответствуют [20].

Определение 1. Обозначим через $\mathrm{Mat}_\infty(R)$ кольцо матриц со счётным числом строк и столбцов, у которых вне главной диагонали есть лишь конечное число ненулевых элементов, а также существует такой номер n, что для любого $i \geqslant n$ $r_{ii} = a$, $a \in R$.

Ясно, что $\mathrm{Mat}_\infty(R)$ — это кольцо.

Пусть $A \in \mathrm{GL}_n(R)$. Мы отождествим A с элементом из $\mathrm{Mat}_\infty(R)$ по следующему правилу: матрицу A запишем в левый верхний угол, начиная с позиции (n, n) на диагонали запишем 1, а на всех остальных местах запишем 0.

Сохраним обозначение $\mathrm{GL}_n(R)$ для получившихся подгрупп в $\mathrm{Mat}_\infty(R)$. Ясно, что $\mathrm{GL}_n(R)$ — подгруппы группы обратимых элементов кольца $\mathrm{Mat}_\infty(R)$, а также что для $m \geqslant n$ мы имеем $\mathrm{GL}_n(R) \subseteq \mathrm{GL}_m(R)$.

Определение 2. Положим

$$\mathrm{GL}(R) = \bigcup_{n\geqslant 1} \mathrm{GL}_n(R) \quad (\mathrm{GL}_n(R) \subseteq \mathrm{Mat}_\infty(R)).$$

Это подгруппа группы обратимых элементов кольца $\mathrm{Mat}_\infty(R)$. Назовём её *стабильной линейной группой*.

Для стабильных линейных групп были описаны автоморфизмы: А. С. Аткарская дала описание автоморфизмов стабильных линейных групп $E(R)$ и $\mathrm{GL}(R)$ над коммутативным локальным кольцом R с $1/2$ (см. [1]).

В нашей предыдущей работе [12] было показано, что, несмотря на «бесконечную» размерность стабильной группы, из элементарной эквивалентности двух произвольных колец с единицей следует элементарная эквивалентность стабильных линейных групп над ними, т. е. не требуется выход в логику более высоких порядков. В той же статье было доказано, что из элементарной эквивалентности стабильных линейных групп над коммутативными локальными кольцами с обратимой двойкой следует элементарная эквивалентность соответствующих колец.

В данной работе мы расширяем предыдущий результат для стабильных линейных групп над полями характеристики 2.

2. Доказательство основной теоремы

Рассмотрим группу $\mathrm{GL}(R)$, где R — поле характеристики 2. Обозначим её единицу через E. Для упрощения формул вместо $\exists U\ A = UBU^{-1}$ будем писать $A \sim B$ и говорить, что A *сопряжена* B.

Наша первая цель — выделить формульно подгруппу нашей группы, которая изоморфна $\mathrm{GL}_2(R)$. Для этого мы будем использовать матрицы вида $\mathrm{diag}[1, 1, T]$, где

$$T \sim \mathrm{diag}\left[\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \ldots\right].$$

Первая половина доказательства будет существенно различаться в зависимости от того, извлекаются ли в поле корни третьей степени из единицы.

2.1. Поля, где извлекаются корни из единицы

Пусть поле K имеет характеристику 2 и содержит корни третьей степени из единицы 1, ξ, ξ^2.

Следующая лемма доказывается, например, в [8], но следует она и из классических результатов линейной алгебры.

Лемма 1. *В группе* $\mathrm{GL}_n(K)$ *для любого набора попарно коммутирующих матриц порядка 3 существует базис, в котором они все имеют вид* $\mathrm{diag}[\xi_1, \ldots, \xi_n]$, *где на диагонали стоят корней третьей степени из единицы.*

Ясно, что для конечного набора матриц лемма выполняется и в стабильной линейной группе $\mathrm{GL}(R)$.

Пусть A — множество матриц. Обозначим через $|||A|||$ количество классов сопряжённости в этом множестве.

Лемма 2. *Пусть набор* $D = [d_1, d_2, d_3, \ldots, d_k]$ *элементов из* K *включает* $[\xi, \xi]$ *или* $[\xi, \xi^2]$. *Тогда* $|||\{AB\colon A \sim \mathrm{diag}[D],\ B \sim \mathrm{diag}[D],\ AB = BA\}||| > 2$.

Доказательство. Для доказательства леммы достаточно будет рассмотреть только пару элементов из условия теоремы — остальные можно просто зафиксировать на первых позициях. Также будет достаточно проверить лишь перестановки диагональных элементов.

Рассмотрим сначала случай, когда D включает $[\xi, \xi]$. Будем считать, что этим элементам соответствуют d_{k-1}, d_k. Первые $k-2$ элемента оставляем на месте, при перемножении они будут давать одинаковый набор собственных значений. Тогда возможно получить следующие матрицы:

$$\begin{aligned}
\mathrm{diag}[1,1,\xi,\xi] \cdot \mathrm{diag}[\xi,\xi,1,1] &= \mathrm{diag}[\xi,\xi,\xi,\xi],\\
\mathrm{diag}[1,1,\xi,\xi] \cdot \mathrm{diag}[\xi,1,\xi,1] &= \mathrm{diag}[\xi,1,\xi^2,\xi],\\
\mathrm{diag}[1,1,\xi,\xi] \cdot \mathrm{diag}[1,1,\xi,\xi] &= \mathrm{diag}[1,1,\xi^2,\xi^2].
\end{aligned}$$

В этой записи для простоты чтения опущены $d_1, d_2, d_3, \ldots, d_{k-2}$ и финальные единицы у стабильных матриц. У всех этих матриц различны наборы собственных значений, а значит, они не сопряжены.

Если D включает $[\xi, \xi^2]$, то

$$\begin{aligned}
\mathrm{diag}[1,1,\xi,\xi^2] \cdot \mathrm{diag}[1,1,\xi,\xi^2] &= \mathrm{diag}[1,1,\xi^2,\xi],\\
\mathrm{diag}[1,1,\xi,\xi^2] \cdot \mathrm{diag}[\xi,\xi^2,1,1] &= \mathrm{diag}[\xi,\xi^2,\xi,\xi^2],\\
\mathrm{diag}[1,1,\xi,\xi^2] \cdot \mathrm{diag}[1,\xi^2,\xi,1] &= \mathrm{diag}[1,\xi^2,\xi^2,\xi^2],
\end{aligned}$$

имеем аналогичную ситуацию. □

Из этих двух лемм следует ещё одна лемма.

Лемма 3. *Пусть* $A^3 = E$. *Если* $|||\{BC\colon B \sim A,\ C \sim A,\ CB = BC\}||| = 2$, *то* $A \sim \mathrm{diag}[\xi]$ (*или* $A \sim \mathrm{diag}[\xi^2]$).

Эта лемма даёт способ выделить матрицу, сопряжённую с одной из матриц $\mathrm{diag}[\xi]$, $\mathrm{diag}[\xi^2]$:

$$\begin{aligned}
\varphi(A) := {}& \exists X_1\, \exists X_2\, \exists Y_1\, \exists Y_2\, \forall Z_1\, \forall Z_2\, (A^3 = E) \wedge \neg(A = E) \wedge\\
&\wedge (X_1 \sim X_2 \sim Y_1 \sim Y_2 \sim A) \wedge (X_1X_2 = X_2X_1) \wedge (Y_1Y_2 = Y_2Y_1) \wedge\\
&\wedge \Big(\big((Z_1 \sim A) \wedge (Z_2 \sim A) \wedge (Z_1Z_2 = Z_2Z_1)\big) \to\\
&\to \big((Z_1Z_2 \sim Y_1Y_2) \vee (Z_1Z_2 \sim X_1X_2)\big)\Big).
\end{aligned} \tag{1}$$

Пусть эта формула истинна для A. Будем считать, что $A \sim \mathrm{diag}[\xi]$. Это возможно получить с помощью замены обозначений $\xi^2 \to \xi'$, $\xi \to \xi'^2$. Тогда $A^2 \sim \mathrm{diag}[\xi^2]$.

Рассмотрим формулу

$$\psi(B) := \exists X_1\, \exists X_2\ (X_1 \sim A) \wedge (X_2 \sim A^2) \wedge (X_1X_2 = X_2X_1) \wedge (X_1X_2 = B) \wedge \neg\varphi(B).$$

Если эта формула истинна для B, то $B \sim \mathrm{diag}[\xi, \xi^2]$.

Пусть $X_1 \sim X_2 \sim A$, $X_1X_2 = X_2X_1$. Тогда можно считать, что выбран такой базис, что $X_1 = \mathrm{diag}[\xi, 1, \ldots]$, $X_2 = \mathrm{diag}[1, \xi, \ldots]$.

Рассмотрим формулу

$$\theta(C) := (CX_1 = X_1C) \wedge (CX_2 = X_2C) \wedge (C \sim B) \wedge \bigwedge_i \neg\varphi(BX_i) \wedge \bigwedge_i \neg\varphi(BX_i^2).$$

Если эта формула истинна для матрицы $C = (c_{ij})$, то, в силу того что C коммутирует с X_i, $i = 1, 2$, мы имеем $c_{1j} = c_{i1} = 0$, $i, j > 1$; $c_{2j} = c_{i2} = 0$, $i, j > 2$. Это матрица порядка 3, значит, $c_{11}^3 = 1$, $c_{22}^3 = 1$. Предположим, что $c_{11} \neq 1$. Тогда $c_{11} = \xi$ или $c_{11} = \xi^2$. Предположим, не умаляя общности, что $c_{11} = \xi$. Тогда после домножения на X_1 матрица станет удовлетворять формуле φ, что противоречит нашей формуле. Значит, $c_{11} = 1$, аналогично $c_{22} = 1$. Тогда $C = \mathrm{diag}[1, 1, T]$, где $T \sim \mathrm{diag}[\xi, \xi^2]$.

Лемма 4.

$$\mathrm{diag}[\xi, \xi^2] \sim \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Доказательство. Для доказательства требуется найти собственные числа матрицы. Характеристический многочлен имеет вид $P(\lambda) = \lambda^2 + \lambda + 1$. Подставив в характеристический многочлен ξ, получим $P(\xi) = \xi^2 + \xi + 1$. Заметим, что $P(\xi) = \xi P(\xi)$, а значит,

$$P(\xi) + \xi P(\xi) = 0 \Longrightarrow P(\xi)(1 + \xi) = 0 \Longrightarrow P(\xi) = 0.$$

Аналогично для ξ^2. Значит, ξ (как и ξ^2) является корнем характеристического уравнения. $\square$

2.2. Поля, где не извлекаются корни из единицы

Пусть K — поле характеристики 2 без нетривиальных корней третьей степени из единицы.

Лемма 5. *В группе $\mathrm{GL}_n(K)$ любой набор коммутирующих матриц порядка 3 имеет в некотором базисе общий блочно-диагональный вид, при этом каждый блок — это блок из набора $E_{11} + E_{12} + E_{21}$, $E_{22} + E_{12} + E_{21}$, $E_{11} + E_{22}$.*

Данная лемма доказана в [8] для случая GL_n, однако она очевидно верна и для GL.

Пусть $T := E_{11} + E_{12} + E_{21}$. Обозначим $D_k = \mathrm{diag}[\underbrace{T, T, \ldots, T, T}_{k}, 1, \ldots]$.

Лемма 6. *Для* $k > 1$ *имеет место*

$$|||\{AB\colon A \sim D_k,\ B \sim D_k,\ AB = BA\}||| > 3.$$

Доказательство. Достаточно будет рассмотреть только два блока T, которые есть в блочно-диагональном виде матрицы A, как следует из условия. Перестановкой этих двух блоков получаем

$$\begin{aligned}
&\mathrm{diag}[E,E,T,T]\cdot\mathrm{diag}[T,T,E,E] = \mathrm{diag}[T,T,T,T],\\
&\mathrm{diag}[E,E,T,T]\cdot\mathrm{diag}[E,E,T^2,T^2] = \mathrm{diag}[E,E,E,E],\\
&\mathrm{diag}[E,E,T,T]\cdot\mathrm{diag}[E,E,T,T] = \mathrm{diag}[E,E,T^2,T^2],\\
&\mathrm{diag}[E,E,T^2,T]\cdot\mathrm{diag}[E,T,T^2,E] = \mathrm{diag}[E,T,T,T],
\end{aligned}$$

где E — единичная матрица размера 2×2. Как следует из доказательства леммы 4, $T^2 \sim T$. □

Из этой леммы мы получаем формулу, выделяющую матрицы, сопряжённые D_1:

$$\begin{aligned}
\varphi'(A) :=\ &\exists X_1\,\exists X_2\,\exists Y_1\,\exists Y_2\,\forall Z_1\,\forall Z_2\ (A^3 = E)\wedge\neg(A = E)\wedge\\
&\wedge(X_1\sim X_2\sim Y_1\sim Y_2\sim A)\wedge(X_1X_2 = X_2X_1)\wedge(Y_1Y_2 = Y_2Y_1)\wedge\\
&\wedge\Big(\big((Z_1\sim A)\wedge(Z_2\sim A)\wedge(Z_1Z_2 = Z_2Z_1)\big)\to\\
&\to\big((Z_1Z_2\sim X_1X_2)\vee(Z_1Z_2\sim Y_1Y_2)\vee(Z_1Z_2\sim E)\big)\Big).
\end{aligned}\tag{2}$$

Лемма 7. *Пусть матрица* $A = (a_{ij})$ *коммутирует с матрицей*

$$G_k = \mathrm{diag}[\underbrace{1,1,\ldots,1}_{k-1},T,1,1\ldots],\quad \text{где}\ \ k\geqslant 1.$$

Тогда

1) *если* $j+1<k$ *или* $k+1<j$, *то*

$$\begin{pmatrix} a_{j,k} & a_{j,k+1}\\ a_{j+1,k} & a_{j+1,k+1}\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix};$$

2) *если* $j+1<k$ *или* $k+1<j$, *то*

$$\begin{pmatrix} a_{k,j} & a_{k,j+1}\\ a_{k+1,j} & a_{k+1,j+1}\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix};$$

3) *имеем*

$$\begin{pmatrix} a_{k,k} & a_{k,k+1}\\ a_{k+1,k} & a_{k+1,k+1}\end{pmatrix} = \begin{pmatrix}a & b\\ b & a+b\end{pmatrix}$$

для некоторых a, b.

Доказательство. Пусть A коммутирует с G_k и $B = (b_{ij}) = AG_k$. Рассмотрим

$$\begin{pmatrix} b_{j,k} & b_{j,k+1} \\ b_{j+1,k} & b_{j+1,k+1} \end{pmatrix}.$$

С одной стороны (при домножении на G_k слева),

$$\begin{pmatrix} b_{j,k} & b_{j,k+1} \\ b_{j+1,k} & b_{j+1,k+1} \end{pmatrix} = \begin{pmatrix} a_{j,k} & a_{j,k+1} \\ a_{j+1,k} & a_{j+1,k+1} \end{pmatrix}.$$

С другой стороны (при домножении на G_k справа),

$$\begin{pmatrix} b_{j,k} & b_{j,k+1} \\ b_{j+1,k} & b_{j+1,k+1} \end{pmatrix} = \begin{pmatrix} a_{j,k} + a_{j,k+1} & a_{j,k} \\ a_{j+1,k} + a_{j+1,k+1} & a_{j+1,k} \end{pmatrix}.$$

Тогда

$$\begin{pmatrix} a_{j,k} & a_{j,k+1} \\ a_{j+1,k} & a_{j+1,k+1} \end{pmatrix} = \begin{pmatrix} a_{j,k} + a_{j,k+1} & a_{j,k} \\ a_{j+1,k} + a_{j+1,k+1} & a_{j+1,k} \end{pmatrix}.$$

Отсюда следует (из равенства левых столбцов), что $a_{j,k+1} = a_{j+1,k+1} = 0$. Но тогда из равенства правых столбцов следует равенство нулю остальных элементов.

Второе утверждение доказывается абсолютно аналогично первому.

Докажем третье утверждение. Мы имеем

$$\begin{pmatrix} a_{k,k} + a_{k+1,k} & a_{k,k+1} + a_{k+1,k+1} \\ a_{k,k} & a_{k,k+1} \end{pmatrix} = \begin{pmatrix} a_{k,k} + a_{k,k+1} & a_{k,k} \\ a_{k+1,k} + a_{k+1,k+1} & a_{k+1,k} \end{pmatrix}.$$

Отсюда следует, что $b := a_{k,k+1} = a_{k+1,k}$, $a := a_{kk}$, и тогда $a_{k+1,k+1} = a + b$. $\square$

Пусть X — матрица, выделяемая формулой φ'. Рассмотрим формулу

$$\theta'(C) := (CX = XC) \wedge (C \sim X) \wedge (CX \neq E) \wedge (CX^2 \neq E).$$

Пусть C удовлетворяет этой формуле. Будем считать, что выбран базис, в котором X имеет вид G_1. Тогда по лемме 7 $c_{1j} = c_{i1} = 0$, $c_{2j} = c_{i2} = 0$, $i, j > 2$. Также

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}.$$

При этом

$$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

или

$$\begin{pmatrix} a^3 + ab^2 + b^3 & a^2b + ab^2 \\ a^2b + ab^2 & a^3 + a^2b + b^3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Из этого следует, что $a^2b + ab^2 = ab(a+b) = 0$. Поскольку в полях нет делителей нуля, возможны лишь три случая:

1) $b = 0$; тогда

$$a^3 = 1 \Longrightarrow a = 1;$$

2) $a = 0$; тогда
$$b^3 = 1 \Longrightarrow b = 1;$$

3) $a = b$; тогда
$$a^3 + ab^2 + b^3 = 1 \Longrightarrow a^3 + a^3 + a^3 = 1 \Longrightarrow a^3 = 1 \Longrightarrow a = b = 1.$$

Первый случай соответствует единичной матрице. Оставшиеся два случая соответствуют
$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = T$$
и
$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = T^2.$$
Эти два случая невозможны, поскольку иначе матрица C становилась бы единичной при домножении на X или X^2, а это запрещает формула θ'. Тем самым мы получили, что матрица C имеет вид $C = \operatorname{diag}[1, 1, T']$, где $T' \sim D_1$.

2.3. Элементарная определимость $\mathrm{GL}_2(K)$ и основная теорема

Пусть формула θ выделяет матрицы вида $\operatorname{diag}[1, 1, T]$, где
$$T \sim \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$
Выделим с их помощью $\mathrm{GL}_2(K)$. Заметим, что матрицы G_k, $k > 2$, находятся среди выделяемых такой формулой. Пусть матрица M коммутирует с G_{2k+1}, $k = 1, 2, 3, \ldots$. Тогда матрица M имеет вид
$$M = \operatorname{diag}[M_0, M_1, M_2, M_3, M_4, \ldots, M_k],$$
где M_0 — произвольная матрица из $\mathrm{GL}_2(K)$, а матрицы M_i, $i > 0$, имеют вид
$$M_i = \begin{pmatrix} a_i & b_i \\ b_i & a_i + b_i \end{pmatrix}.$$

Пусть дополнительно матрица M коммутирует с G_{2k+2}, $k = 1, 2, 3, \ldots$. Тогда матрица M имеет вид $M = \operatorname{diag}[M_0, a_1, M'_1, M'_2, M'_3, M'_4, \ldots, M'_{k'}]$, где матрицы M'_i имеют вид
$$M'_i = \begin{pmatrix} a'_i & b'_i \\ b'_i & a'_i + b'{}^{\text{‘}}{}_i \end{pmatrix}.$$
Из сопоставления блочной структуры разных представлений M получаем
$$M = \operatorname{diag}[M_0, M_1, M_2, M_3, M_4, \ldots, M_k] = \operatorname{diag}[M_0, a_1, M'_1, M'_2, M'_3, M'_4, \ldots, M'_{k'}],$$
т. е. $b_i = b'_i = 0$, и тогда $a_i = a'_i$, а также $a'_i = a_{i+1}$. Из этого следует, что $a_i = a_{i+1}$ для любого i. Но тогда из определения стабильной линейной группы

следует, что $a_i = 1$, иначе было бы бесконечное число отличных от единицы элементов на диагонали.

Тогда мы получаем формулу, которая выделяет множество (подгруппу), изоморфное $\mathrm{GL}_2(K)$:

$$\gamma(M) = \forall C\ \big(\theta(C) \to (MC = CM)\big).$$

Теперь мы готовы доказать основную теорему этой работы.

Теорема 3. *Пусть K_1 и K_2 — поля характеристики 2. Если стабильные линейные группы $\mathrm{GL}(K_1)$ и $\mathrm{GL}(K_2)$ элементарно эквивалентны, то поля K_1 и K_2 также элементарно эквивалентны.*

Доказательство. Пусть $\mathrm{GL}(K_1) \equiv \mathrm{GL}(K_2)$. Так как в предыдущих леммах мы показали, что подгруппа GL_2 элементарно определима в группе GL для поля характеристики 2, то это означает, что $\mathrm{GL}_2(K_1) \equiv \mathrm{GL}_2(K_2)$. По обобщению теоремы Мальцева, доказанному, например, в [10], отсюда следует $K_1 \equiv K_2$. $\square$

Литература

[1] Аткарская А. С. Автоморфизмы стабильных линейных групп над коммутативными локальными кольцами с 1/2 // Фундамент. и прикл. матем. — 2012. — Т. 17, вып. 7. — С. 15—30.

[2] Брагин В., Бунина Е. Элементарная эквивалентность линейных групп над кольцами с конечным числом центральных идемпотентами и над булевыми кольцами // Фундамент. и прикл. матем. — 2013. — Т. 18, вып. 1. — С. 45—55.

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

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

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

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

[7] Бунина Е. И. Изоморфизмы и элементарная эквивалентность групп Шевалле над коммутативными кольцами // Матем. сб. — 2019. — Т. 210, № 8. — С. 3—28.

[8] 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.

[9] Бунина Е. И., Михалёв А. В. Элементарная эквивалентность категорий модулей над кольцами // Фундамент. и прикл. матем. — 2004. — Т. 10, вып. 2. — С. 51—134.

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

[11] Бунина Е. И., Михалёв А. В., Ройзнер М. А. Критерий элементарной эквивалентности групп автоморфизмов и колец эндоморфизмов абелевых p-групп // Докл. РАН. — 2014. — Т. 457, № 1. — С. 11—12.

[12] Бунина Е. И., Михалёв А. В., Соловьёв И. О. Элементарная эквивалентность стабильных линейных групп над локальными коммутативными кольцами с 1/2 // Фундамент. и прикл. матем. — 2016. — Т. 21, вып. 1. — С. 65—78.

[13] Голубчик И. З., Михалёв А. В. Изоморфизмы общей линейной группы над ассоциативными кольцами // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 1983. — № 3. — С. 61—72.

[14] Гончаров С. С. Счётные булевы алгебры и разрешимость. — Новосибирск: Научные книги, 1996.

[15] Мальцев А. И. Об изоморфных матричных представлениях бесконечных групп // Матем. сб. — 1940. — Т. 8 (50). — С. 405—422.

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

[17] Beidar K. I., Mikhalev A. V. On Mal'cev's theorem on elementary equivalence of linear groups // Contemp. Math. — 1992. — Vol. 131, no. 1. — P. 29—35.

[18] Chang C., Keisler H. Model Theory. — North-Holland, 1990.

[19] Golubchik I. Z. Isomorphisms of the general linear group $\mathrm{GL}_n(R)$, $n \geqslant 4$, over an associative ring // Contemp. Math. — 1992. — Vol. 131, no. 1. — P. 123—137.

[20] Hahn A. J., O'Meara O. T. The Classical Groups and K-Theory. — Berlin: Springer, 1989.

[21] Keisler H. J. Ultraproducts and elementary models // Indag. Math. — 1961. — Vol. 23. — P. 477—495.

[22] Kharlampovich O., Myasnikov A. Elementary theory of free non-Abelian groups // J. Algebra. — 2006. — Vol. 302. — P. 451—552.

[23] Sela Z. Diophantine geometry over groups. VI. The elementary theory of a free group // Geom. Funct. Anal. — 2016. — Vol. 16, no. 3. — P. 707—730.

[24] Sela Z. Diophantine geometry over groups and the elementary theory of free and hyperbolic groups // Proc. of the Int. Congress of Mathematicians. Vol. II (Beijing, 2002). — Beijing, 2002. — P. 87—92.

[25] Shelah S. Every two elementarily equivalent models have isomorphic ultrapowers // Israel J. Math. — 1971. — Vol. 10. — P. 224—233.

[26] Stephenson W. Lattice isomorphism between modules // J. London Math. Soc. — 1969. — Vol. 1. — P. 177—188.

[27] Szmielew W. Elementary properties of Abelian groups // Fund. Math. — 1955. — Vol. 41. — P. 203—271.

[28] Tolstykh V. Elementary equivalence of infinite-dimensional classical groups // Ann. Pure Appl. Logic. — 2000. — P. 105. — P. 103—156.