ЧЕБЫШЕВСКИЙ СБОРНИК
Том 24. Выпуск 5.

УДК 512.55 DOI 10.22405/2226-8383-2023-24-5-85-111

Инволюции в алгебре верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей

И. А. Кульгускин

Кульгускин Иван Александрович — аспирант, Казанский (Приволжский) федеральный университет (г. Казань).
e-mail: ivan-kull@rambler.ru

Аннотация

В статье исследована классификация с точностью до эквивалентности инволюций в алгебре верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей.

Описание инволюций в алгебрах представляет собой одну из классических задач теории колец. Стандартными примерами инволюций является транспонирование в матричной алгебре и сопряжение в поле комплексных чисел и алгебре кватернионов.

В случае, когда поле P имеет характеристику отличную от двух, полное описание инволюций с точности до их эквивалентности в алгебре $T_n(P)$ для любого натурального числа n, было плучено в [15]. В работе [3] исследованы инволюции в алгебре верхнетреугольных матриц над коммутативными кольцами. Если кольцо является полем характеристики 2 или булевым кольцом, то были найдены необходимые и достаточные условия конечности числа классов эквивалентности инволюций.

Данная статья является продолжением работы [3]. В статье [3], в частности, было найдено число классов эквивалентности инволюций в алгебрах верхнетреугольных матриц над кольцом целых чисел. В связи с этим результатом естественной является задача об описании инволюций с точностью до их эквивалентности в алгебрах верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей, которой посвящена настоящая работа. В работе найдено число классов эквивалентности инволюций в таких алгебрах и на примерах проиллюстрирован способ нахождения представителей в каждом классе эквивалентности. При получении основных результатов в настоящей работе существенно используется аппарат теории уравнений Пелля.

Ключевые слова: инволюции, алгебра верхнетреугольных матриц, кольцо целых алгебраических чисел квадратичных полей.

Библиография: 24 названия.

Для цитирования:
И. А. Кульгускин. Инволюции в алгебре верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей // Чебышевский сборник, 2023, т. 24, вып. 5, с. 85–111.

CHEBYSHEVSKII SBORNIK
Vol. 24. No. 5.

UDC 512.55 DOI 10.22405/2226-8383-2023-24-5-85-111

Involutions in the algebra of upper triangular matrices over the ring of algebraic integers of quadratic fields

I. A. Kulguskin

Kulguskin Ivan Alexandrovich — postgraduate student, Kazan (Volga Region) Federal University (Kazan).
e-mail: ivan-kull@rambler.ru

Abstract

The article investigates the classification with precision up to equivalence of involutions in the algebra of upper triangular matrices over the ring of integers of algebraic numbers of quadratic fields.

The description of involutions in algebras represents one of the classical problems of ring theory. Standard examples of involutions are transposition in matrix algebra and conjugation in the field of complex numbers and the algebra of quaternions.

In the case where the field P has a characteristic different from two, a complete description of involutions with precision up to their equivalence in the algebra $T_n(P)$ for any natural number n was obtained in [15]. In this work [3] involutions in the algebra of upper triangular matrices over commutative rings are studied. If the ring is a field of characteristic 2 or a Boolean ring, then necessary and sufficient conditions for the finiteness of the number of equivalence classes of involutions were found.

This article is a continuation of the work of [3]. In the article [3], in particular, the number of equivalence classes of involutions in the algebras of upper triangular matrices over the ring of integers was found. In this regard, the natural result is the problem of describing involutions with precision up to their equivalence in algebras of upper triangular matrices over the ring of algebraic integers of quadratic fields, to which this work is devoted. In the work, the number of equivalence classes of involutions in such algebras is found and the method of finding representatives in each equivalence class is illustrated with examples. Upon receipt the main results in this work, the apparatus of the theory of Pell's equations is significantly used.

Keywords: involutions, the algebra of upper triangular matrices, the ring of algebraic integers of quadratic fields.

Bibliography: 24 titles.

For citation:
I. A. Kulguskin, 2023, "Involutions in the algebra of upper triangular matrices over the ring of algebraic integers of quadratic fields" , *Chebyshevskii sbornik*, vol. 24, no. 5, pp. 85–111.

1. Введение

Пусть R – коммутативное кольцо и $\mathbb{A}$ – произвольная R-алгебра.

R-линейное отображение $\gamma : \mathbb{A} \to \mathbb{A}$ называется *инволюцией*, если $\forall a, b \in \mathbb{A}\ \gamma(ab) = \gamma(b)\gamma(a)$ и $\gamma^2(a) = a$. Две инволюции γ, δ алгебры $T_n(R)$ называются *эквивалентными*, если существует изоморфизм $\varphi : (T_n(R), \gamma) \to (T_n(R), \delta)$ такой, что для любой матрицы $A \in T_n(R)$ $\varphi(\gamma(A)) = \delta(\varphi(A))$.

Описание инволюций в алгебрах представляет собой одну из классических задач теории колец. Стандартными примерами инволюций является транспонирование в матричной алгебре и сопряжение в поле комплексных чисел и алгебре кватернионов. Систематическое изучение инволюций в центральных простых алгебрах впервые было предпринято Альбертом в 30-е годы прошлого века. Многие его результаты нашли отражение в монографии [6]. К настоящему времени теория инволюций в центральных простых алгебрах достаточно глубоко развита и многие ее результаты представлены в монографиях [12], [11].

При классификации инволюций с точностью до их эквивалентности в алгебре $\mathbb{A}$ важным является описание группы внешних автоморфизмов $\mathrm{Out}(\mathbb{A})$ алгебры $\mathbb{A}$. В работе [15] был получен критерий эквивалентности двух инволюций произвольной алгебры $\mathbb{A}$ в случае, когда $\mathrm{Out}(\mathbb{A})$ является единичной группой. С помощью этого критерия в этой работе было показано, что в случае, когда характеристика поля F отлична от двух, любая инволюция алгебры верхнетреугольных матриц над F эквивалентна либо симплектической, либо ортогональной. Таким образом, при изучении инволюций в различных классах матричных колец важным является нахождение условий, при которых все автоморфизмы таких колец являются внутренними. Автоморфизмы колец формальных матриц и условия, при которых у колец формальных верхнетреугольных матриц и близких к ним колец все автоморфизмы являются внутренними, в последнее время были изучены в работах Крылова П.А., Норбосамбуева Ц.Д. и Туганбаева А.А. (см. [1, 2, 13]).

Важным частным случаем алгебр верхнетреугольных формальных матриц являются алгебры инцидентности над частично-упорядоченными множествами. Исследование инволюций в алгебрах инцидентности и их обобщениях в последнее время получило большое развитие (см. [14, 7, 9, 8, 10]). Однако, классификации инволюций с точностью до их эквивалентности в таких алгебрах была получена только в случае, когда характеристика основного поля отлична от двух.

В статье [3] исследованы инволюции в алгебре верхнетреугольных матриц над полями характеристики 2 . Как оказалось, существуют примеры алгебр верхнетреугольных матриц, у которых имеются бесконечное число классов эквивалентностей инволюций. Также в данной работе были исследованы с точностью до эквивалентности инволюции первого рода в алгебре верхнетреугольных матриц над коммутативными кольцами, у которых 2 не обязательно является обратимой. Если кольцо является полем характеристики 2 или булевым кольцом, то были найдены необходимые и достаточные условия конечности числа классов эквивалентности инволюций.

Нетривиальной задачей и хорошим дополнением к развитой теории работы [3] служит изучение проблемы классификации инволюций в алгебре верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей. В ходе описания инволюций в вышеупомянутой алгебре были найдены эквивалентные формулировки условий в рамках теории уравнений Пелля [5].

2. Предварительные сведения

Существенным условием при изучении вопроса классификаций инволюций с точностью до их эквивалентности над мутативными кольцами, у которых двойка не является обратимой, в работе [3] является поднимаемость всех обратимых элементов кольца $R/2R$ до обратимых элементов кольца R по модулю идеала $2R$. В общем это условие может не выполнятся. К примеру, если взять $R = \mathbb{Z}[\sqrt{-5}]$, то нетрудно видеть, что в фактор кольце $R/2R$ элемент $\sqrt{-5} + 2R$ в квадрате дает единицу фактор кольца, а значит обратим. В то же время, из стандарной нормы на $\mathbb{Z}[\sqrt{-5}]$ напрямую следует, что $\sqrt{-5} + 2R$ нельзя поднять до обратимого элемента R. Тем не менее, в ряде случаев эту проблему можно обойти. Заметим, что в определении отношения

$\sim_{odd}$ (см. [3]) участвуют не сами обратимые элементы, а их квадраты. Поэтому в Следствии 4 [3] при четном n достаточно требовать поднимаемости квадратов обратимых элементов, что уже выполняется для кольца $\mathbb{Z}[\sqrt{-5}]$.

Следующие утверждения дают полное описание инволюций в алгебре верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей. Их доказательство будет представлено в последующих двух параграфах.

Пусть $n \in \mathbb{N}$, $d \in \mathbb{Z}$ – бесквадратное целое и R – кольцо целых алгебраических чисел $\mathbb{Q}[\sqrt{d}]$.

Теорема 1. *Пусть $d \equiv 3(\mathrm{mod}4)$. Тогда при $n = 2k+1$ – нечетном в алгебре $T_{2k+1}(R)$ имеется ровно $k+1$ классов эквивалентности инволюций и при $n = 2k$ – четном:*

1. *если уравнение $x^2 - dy^2 = 1$, где x – четное, y – нечетное, не разрешимо в целых числах, то в алгебре $T_{2k}(R)$ имеется ровно $3k^2+2$ классов эквивалентности инволюций;*

2. *если уравнение $x^2 - dy^2 = 1$, где x – четное, y – нечетное, разрешимо в целых числах, то в алгебре $T_{2k}(R)$ имеется ровно k^2+k+2 классов эквивалентности инволюций.*

Теорема 2. *Пусть $d \equiv 2(\mathrm{mod}4)$. Тогда при $n = 2k+1$ – нечетном в алгебре $T_{2k+1}(R)$ имеется ровно $k+1$ классов эквивалентности инволюций и при $n = 2k$ – четном:*

1. *если уравнение $x^2 - dy^2 = -1$, где x, y – нечетные, не разрешимо в целых числах, то в алгебре $T_{2k}(R)$ имеется ровно $3k^2+2$ классов эквивалентности инволюций;*

2. *если уравнение $x^2 - dy^2 = -1$, где x, y – нечетные, разрешимо в целых числах, то в алгебре $T_{2k}(R)$ имеется ровно k^2+k+2 классов эквивалентности инволюций.*

Теорема 3. *Пусть $d = 4t+1, t \in \mathbb{Z}$. Тогда при $n = 2k+1$ – нечетном в алгебре $T_{2k+1}(R)$ все инволюции попарно эквивалентны и при $n = 2k$ – четном:*

1. *если t – четное, то в алгебре $T_{2k}(R)$ имеется ровно $(k+1)^2$ классов эквивалентности инволюций;*

2. *если t – нечетное и уравнение $x^2 - dy^2 = \pm 4$, где x, y – нечетные, не разрешимо в целых числах, то в алгебре $T_{2k}(R)$ имеется ровно $3k+2$ классов эквивалентности инволюций;*

3. *если t – нечетное и уравнение $x^2 - dy^2 = \pm 4$, где x, y – нечетные, разрешимо в целых числах, то в алгебре $T_{2k}(R)$ имеется ровно $(k+1)^2+1$ классов эквивалентности инволюций.*

В дальнейшем нам потребуется техническое утверждение.

Пусть R – коммутативное кольцо и $U \subset R/2R$ – подгруппа обратимых элементов фактор кольца, которые поднимаются по модулю $2R$ и $k \in \mathbb{N}$. Аналогично отношениям $\sim_{even}$ и $\sim_{odd}$, введенным в [3], можно ввести следующие два новых отношения эквивалентности на $(R/2R)^k$. Пусть $z = (z_1, \ldots, z_k), h = (h_1, \ldots, h_k) \in (R/2R)^k$. Положим

1. $z \sim_{even,U} h \Leftrightarrow$ существуют $\lambda \in U$ и наборы $c_{ii} \in U$, $c_{ij} \in R/2R$, такие что

$$h_i = \lambda \left(c_{ii}^2 z_i + \sum_{j=1}^{i-1} c_{ij}^2 z_j \right);$$

2. $z \sim_{odd,U} h \Leftrightarrow$ существуют наборы $c_{ii} \in U$, $e_i, c_{ij} \in R/2R$, такие что

$$h_i = c_{ii}^2 z_i + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 z_j.$$

Теорема 4. *Пусть R – коммутативное кольцо, $2 \notin U(R)$, $n, k \in \mathbb{N}$ и $n > 1$. Через Θ обозначим множество классов эквивалентности инволюций γ_B алгебры $T_n(R)$, таких что $B^* = B$. Тогда*

1. *Если $n = 2k+1$ нечетно, то $|\Theta| = \left|(R/2R)^k/\sim_{odd,U}\right|$;*
2. *Если $n = 2k$ четно, то $|\Theta| = \left|(R/2R)^k/\sim_{even,U}\right|$.*

Доказательство. Пусть $z = (z_1, \ldots, z_k), h = (h_1, \ldots, h_k) \in R^k$ и $\overline{z} = (\overline{z_1}, \ldots, \overline{z_k})$, $\overline{h} = (\overline{h_1}, \ldots, \overline{h_k}) \in (R/2R)^k$. Докажем, что $z \sim_{odd} h$ тогда и только тогда, когда $\overline{z} \sim_{odd,U} \overline{h}$.

Действительно, если $z \sim_{odd} h$, то существуют наборы $c_{ii} \in U(R)$, $e_i, c_{ij} \in R$, такие что

$$h_i - \left(c_{ii}^2 z_i + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 z_j \right) \in 2R.$$

Следовательно,

$$\overline{h_i} = \overline{c_{ii}}^2 \overline{z_i} + \overline{e_i}^2 + \sum_{j=1}^{i-1} \overline{c_{ij}}^2 \overline{z_j} \text{ в } R/2R.$$

И значит, $\overline{z} \sim_{odd,U} \overline{h}$.

Обратно. Допустим, что $\overline{z} \sim_{odd,U} \overline{h}$. Следовательно, существуют наборы $\overline{c_{ii}} \in U$, $\overline{e_i}, \overline{c_{ij}} \in R/2R$, такие что

$$\overline{h_i} = \overline{c_{ii}}^2 \overline{z_i} + \overline{e_i}^2 + \sum_{j=1}^{i-1} \overline{c_{ij}}^2 \overline{z_j}.$$

В силу того, что $U \subset R/2R$ – подгруппа обратимых элементов фактор кольца, которые поднимаются по модулю $2R$, мы имеем

$$h_i - \left(c_{ii}^2 z_i + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 z_j \right) \in 2R.$$

Поэтому $z \sim_{odd} h$. Далее результат следует из предложения 2 [3]. Аналогично доказывается, что $z \sim_{even} h$ тогда и только тогда, когда $\overline{z} \sim_{even,U} \overline{h}$. □

3. Классификация инволюций при $d \equiv 2, 3 (\mathrm{mod} 4)$

Напомним некоторые определения, которые понадобятся нам для дальнейшего изложения.

Пусть A — кольцо, x — произвольный элемент поля F, содержащего A.

Definition 1. *Элемент x называется целым над A, если он удовлетворяет некоторому уравнению*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

с коэффициентами из кольца A.

Definition 2. *Целым замыканием кольца A в поле F называется множество тех элементов поля F, которые целы над A.*

Несложно показать, что целое замыкание кольца A в поле F также является кольцом.

Definition 3. *Целое замыкание кольца $\mathbb{Z}$ в числовом поле K называется кольцом целых алгебраических чисел этого поля и обозначается I_K.*

Следующее утверждение показывает, что наше исследование будет распадаться на несколько случаев.

Теорема 5 ([4]). *Пусть целое число d отлично от 0 и 1 и не делится на квадрат простого числа и $K = \mathbb{Q}[\sqrt{d}]$. Если $d \equiv 2(\mathrm{mod}4)$ или $d \equiv 3(\mathrm{mod}4)$, то $\left[1, \sqrt{d}\right]$ составляет базис кольца I_K над $\mathbb{Z}$. Если $d \equiv 1(\mathrm{mod}\ 4)$, то таким базисом является система $\left[1, \frac{1+\sqrt{d}}{2}\right]$.*

Учитывая теорему 5, можем ввести следующие обозначения. $\mathbb{Z}[\sqrt{d}] = I_K$, если $d \equiv 2(\mathrm{mod}4)$ или $d \equiv 3(\mathrm{mod}4)$ и $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = I_K$, если $d \equiv 1(\mathrm{mod}4)$.

Случаи, когда $d \equiv 2(\mathrm{mod}\,4)$ и $d \equiv 3(\mathrm{mod}\,4)$ во многом схожи между собой и этот параграф будет посвящен именно им. В следующем параграфе мы разберем отдельно случай, когда $d \equiv 1(\mathrm{mod}4)$.

Пусть d – бесквадратное целое и $d \equiv 2, 3(\mathrm{mod}4)$. Здесь и далее через φ будем обозначать элемент $\varphi = \sqrt{d} \in R$. Также введем обозначения $R = \mathbb{Z}[\sqrt{d}]$, $R/2R = \{\overline{0}, \overline{1}, \overline{\varphi}, \overline{\varphi+1}\}$, где под $\overline{r}$ мы понимаем образ элемента $r \in R$ под действием естественного гомоморфизма $R \to R/2R$; U – подгруппа обратимых элементов фактор кольца $R/2R$, которые поднимаются по модулю $2R$.

Лемма 1. *Если $d \equiv 2, 3(\mathrm{mod}4)$, то $R/2R \cong \mathbb{Z}_2[x]/(x^2)$.*

Доказательство. Покажем, что квадрат произвольного элемента в $R/2R$ равен $\overline{1}$ или $\overline{0}$, причем квадрат обратимого элемента равен $\overline{1}$. Имеем $R/2R = \{\overline{0}, \overline{1}, \overline{\varphi}, \overline{\varphi+1}\}$.

Если $d \equiv 2(\mathrm{mod}4)$, т.е. $d = 4l + 2, l \in \mathbb{Z}$, то:

$$\overline{\varphi^2} = \overline{d} = \overline{4l+2} = \overline{0};$$

$$\overline{(\varphi+1)^2} = \overline{1 + 2\varphi + \varphi^2} = \overline{1+\varphi^2} = \overline{1}.$$

Если $d \equiv 3(\mathrm{mod}4)$, т.е. $d = 4v + 3, v \in \mathbb{Z}$, то:

$$\overline{\varphi^2} = \overline{d} = \overline{4v+3} = \overline{1};$$

$$\overline{(\varphi+1)^2} = \overline{1 + 2\varphi + \varphi^2} = \overline{1+1} = \overline{0}.$$

Теперь изоморфизм очевиден. □

Для начала рассмотрим, что будет при нечетной размерности матриц, а именно классифицируем инволюции в алгебре $T_{2k+1}(R)$.

Напомним, что по определению эквивалентности векторов $z = (z_1, \ldots, z_k)$, $h = (h_1, \ldots, h_k) \in (R/2R)^k$

$$z \sim_{odd,U} h \Leftrightarrow \exists\ c_{ii} \in U, e_{ii}, c_{ij} \in R/2R \text{ такие, что}$$

$$h_i = c_{ii}^2 z_i + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 z_j.$$

Так как в силу леммы 1 $c_{ii}^2 = \overline{1}$, следовательно определение эквивалентных векторов z и h мы можем переписать в виде:

$$h_i = z_i + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 z_j.$$

Предложение 1. *Пусть* $a = (a_1, \ldots, a_k) \in (R/2R)^k$ *и* θ *– нулевой вектор из* $(R/2R)^k$. *Тогда* $a \sim_{odd,U} \theta \Leftrightarrow \forall\ 1 \leqslant i \leqslant k\ a_i \in \{\overline{0}, \overline{1}\}$.

Доказательство. ($\Rightarrow$) Пусть $a \sim_{odd,U} \theta$, тогда для любого индекса $1 \leqslant i \leqslant k$ имеем

$$a_i = \overline{0} + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0} = e_i^2.$$

По лемме 1 $e_i^2 \in \{\overline{0}, \overline{1}\}$.

($\Leftarrow$) Пусть теперь $a_i \in \{\overline{0}, \overline{1}\}, 1 \leqslant i \leqslant k$. Тогда положим $e_i = a_i, e_i \in R/2R$ и заметим, что

$$a_i = e_i^2 = \overline{0} + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0},$$

для любых $c_{ij} \in R/2R$. Следовательно, $a \sim_{odd,U} \theta$. $\square$

Лемма 2. *Пусть* $a = (a_1, \ldots, a_k), b = (b_1, \ldots, b_k) \in (R/2R)^k$ *и* $a \not\sim_{odd,U} \theta, b \not\sim_{odd,U} \theta$. *Если* $a \sim_{odd,U} b$, *то* $\exists\ s, 1 \leqslant s \leqslant k\ a_s, b_s \notin \{\overline{0}, \overline{1}\}$ *и* $\forall\ i < s\ a_i, b_i \in \{\overline{0}, \overline{1}\}$.

Доказательство. Так как $a \not\sim_{odd,U} \theta$ и $b \not\sim_{odd,U} \theta$, то по Предложению 1 существует минимальный индекс $1 \leqslant m \leqslant k$ такой, что $a_m \notin \{\overline{0}, \overline{1}\}$ и существует минимальный индекс $1 \leqslant n \leqslant k$ такой, что $b_n \notin \{\overline{0}, \overline{1}\}$. Докажем, что $m = n$.

Допустим $m < n$. Тогда так как $a \sim_{odd,U} b$, то

$$a_m = b_m + e_m^2 + \sum_{j=1}^{m-1} c_{mj}^2 b_j.$$

Но $m < n$, значит для любого индекса $1 \leqslant f \leqslant m$ $b_f \in \{\overline{0}, \overline{1}\}$. Тогда левая часть равенства не принадлежит множеству $\{\overline{0}, \overline{1}\}$, а правая - принадлежит множеству $\{\overline{0}, \overline{1}\}$. Данное противоречие завершает доказательство. $\square$ Для каждого s от 1 до k положим

$$h_s = (\overline{h_1}, \ldots, \overline{h_s}, \ldots, \overline{h_k}) \in (R/2R)^k,$$

где $\overline{h_s} = \overline{\varphi}$, а все остальные элементы равны $\overline{0}$.

По предложению 1 $h_s \not\sim_{odd,U} \theta$ и по Лемме 2 $h_s \not\sim_{odd,U} h_{s_1}$, если $s \neq s_1$.

Предложение 2. *Пусть* $a = (a_1, \ldots, a_k) \in (R/2R)^k$ *и* $1 \leqslant s \leqslant k$. *Тогда* $a \sim_{odd,U} h_s \Leftrightarrow a_s \in \{\overline{\varphi}, \overline{\varphi + 1}\}$ *и* $\forall\ i < s\ a_i \in \{\overline{0}, \overline{1}\}$.

Доказательство. ($\Leftarrow$) Так как $\overline{h_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, положив $e_i = a_i, e_i \in R/2R$, имеем

$$a_i = e_i^2 = \overline{h_i} + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 \overline{h_j},$$

для любых $c_{ij} \in R/2R$.

Выберем произвольный элемент a_m, где $s < m \leqslant k$ и покажем, что будет выполняться равенство

$$a_m = \overline{h_m} + e_m^2 + \sum_{j=1}^{m-1} c_{mj}^2 \overline{h_j},$$

для некоторых $e_m, c_{mj} \in R/2R$. Действительно, выберем элементы $e_m, c_{ms} \in R/2R$ так, чтобы выполнялось равенство $a_m = e_m^2 + c_{ms}^2 \overline{h_s}$. Нетрудно убедиться, что такие элементы существуют для любого значения a_m. Теперь заметим, что

$$a_m = e_m^2 + c_{ms}^2 \overline{h_s} = \overline{h_m} + e_m^2 + \sum_{j=1}^{m-1} c_{mj}^2 \overline{h_j},$$

где $c_{mj} = \overline{0}$ при $j \neq s$.

Если же $m = s$, то положив $a_s = \overline{\varphi} + e_s^2, e_s \in R/2R$, имеем

$$a_s = \overline{\varphi} + e_s^2 = \overline{h_s} + e_s^2 = \overline{h_s} + e_s^2 + \sum_{j=1}^{s-1} c_{sj}^2 \overline{h_j},$$

для любых $c_{sj} \in R/2R$.

($\Rightarrow$) Пусть теперь $a \sim_{odd,U} h_s$. Тогда утверждение верно в силу Леммы 2. $\square$ Таким образом, из предложения 1 и предложения 2 следует, что любой вектор в $(R/2R)^k$ эквивалентен либо θ, либо h_s, для некоторого s, следовательно

$$|(R/2R)^k / \sim_{odd,U}| = k + 1.$$

Значит, по Теореме 4 $|\alpha| = k + 1$, где α – множество классов эквивалентности инволюций в $T_{2k+1}(\mathbb{Z}[\sqrt{d}])$.

В алгебре $T_{2k}(R)$, то есть при четной размерности матриц, нам придется разбить случай на $d \equiv 2, 3 (\mathrm{mod} 4)$ на два отдельных. **Далее везде** $d \equiv 3 (\mathrm{mod} 4)$.

Элемент кольца R обратим, тогда и только тогда, когда его норма $|a + b\sqrt{d}| = a^2 - db^2 = \pm 1$. Так как $d \equiv 3 (\mathrm{mod} 4)$, то в $R/2R$ обратимыми элементами являются $\overline{1}$ и $\overline{\varphi}$. Естественно, $\overline{1}$ является обратимым элементом, который поднимается по модулю $2R$.

Лемма 3. *Пусть $d \equiv 3 (\mathrm{mod} 4)$. Тогда все обратимые элементы в $R/2R$ поднимаются по модулю $2R$ тогда и только тогда, когда разрешимо в целых числах уравнение*

$$x^2 - y^2 d = 1, \text{ где } x - \text{ четное}, y - \text{ нечетное}. \qquad (*)$$

Причем, если указанное уравнение не обладает требуемыми решениями, то $U = \{\overline{1}\}$.

Доказательство. Как уже было отмечено выше, $\overline{1}$ является обратимым элементом, который всегда поднимается по модулю $2R$.

Пусть теперь $\overline{\varphi}$ поднимается по модулю $2R$. Элемент $a + b\sqrt{d}$ кольца R принадлежит смежному классу $\overline{\varphi}$ тогда и только тогда, когда a — четное, b — нечетное. Такой элемент будет обратим в кольце R тогда и только тогда, когда разрешимо в целых числах уравнение

$$x^2 - y^2 d = \pm 1, \text{ где } x - \text{ четное}, y - \text{ нечетное}.$$

В этом уравнении перейдем к сравнению по модулю 4. Получим

$$0 - 1 \cdot 3 \equiv \pm 1 (\mathrm{mod} 4).$$

Теперь становится очевидным, что уравнение вида $x^2 - y^2 d = -1$ не имеет решений при x четном и y нечетном. Следовательно, мы можем рассматривать только уравнение

$$x^2 - y^2 d = 1, \text{ где } x - \text{ четное}, y - \text{ нечетное}.$$

Второе утверждение леммы очевидно. $\square$

Следующее утверждение дает критерий разрешимости уравнения (*).

Лемма 4. *Пусть (x_*, y_*) – наименьшее положительное решение уравнения $x^2 - y^2 d = 1$. Тогда уравнение $(*)$ разрешимо тогда и только тогда, когда y_* нечетно.*

Доказательство.

Переходя в уравнении $x^2 - y^2 d = 1$ к сравнению по модулю 4, имеем

$$x^2 + y^2 \equiv 1(\mathrm{mod}4).$$

Таким образом, значения x и y должны иметь разную четность, то есть либо x – четно, y – нечетно, либо x – нечетно, y – четно.

В Следствии 3 [5] были получены рекуррентные соотношения, позволяющие найти все положительные решения уравнения $x^2 - y^2 d = 1$. В частности,

$$y_{n+2} - 2x_* y_{n+1} + y_n = 0,$$

где $y_1 = y_*, y_2 = 2x_* y_*$, а n – натуральное число.

Пусть y_* – четно. Из соотношения, приведенного выше, видно, что y_2 снова будет четным и все последующие y_n также окажутся четными, а значит, уравнение $(*)$ неразрешимо.

Если же y_* – нечетно, то x_* – четно и уравнение $(*)$ разрешимо. □

Отметим, что разрешимость уравнения $(*)$ зависит от значения d. На данный момент не существует общих результатов, описывающих разрешимость уравнения $(*)$ в терминах d. Однако мы можем получить формулу для нахождения некоторых d таких, что уравнение $(*)$ разрешимо.

Пусть $d = u^2 \pm v$, где u и v натуральные числа такие, что $v \mid 2u$. Тогда по Теореме 4 [5] наименьшим положительным решением уравнения $x^2 - y^2 d = 1$ будет

$$x_* = \frac{2u^2}{v} \pm 1,\ y_* = \frac{2u}{v}.$$

Пусть u – нечетное натуральное число и $v_1 \mid u$, тем самым v_1 также нечетно. Тогда при $d = u^2 \pm 2v_1$ получим, что $y_* = \frac{u}{v_1}$ – нечетное число, а значит по лемме 4 уравнение $(*)$ разрешимо. Заметим, что при этом $d \equiv 3(\mathrm{mod}4)$, так как u и v_1 нечетны.

Используя формулу

$$d = u^2 \pm 2v_1, \qquad (\vee)$$

мы можем вычислять только некоторые значения d, при которых уравнение $(*)$ разрешимо

$$d = 3, 7, 11, 15, 23, \ldots$$

Конечно, значение d, полученное при помощи формулы $(\vee)$, не всегда будет бесквадратным числом. При этом, если d будет содержать квадрат какого-либо числа m, то m – нечетно. Значит, мы можем записать d в виде $d = d_1 m^2$, где d_1 – бесквадратное число. А тогда, если (x_0, y_0) – какое-то решение уравнения $(*)$, то (x_0, my_0) – решение $x^2 - d_1 y^2 = 1$ с четным x и нечетным my.

Первым примером d, при котором уравнение $(*)$ не разрешимо является $d = 39$. Несложно убедиться, что наименьшее положительное решение уравнения $x^2 - 39y^2 = 1$ – это пара чисел $(25, 4)$. Действительно, пользуясь теоремой 4 [5] имеем $39 = 6^2 + 3$, следовательно $y_* = \frac{2 \cdot 6}{3} = 4$.

Таким образом, в зависимости от конкретного d в $R/2R$ могут встречаться обратимые элементы, которые поднимаются по модулю $2R$ или которые не поднимаются по модулю $2R$. Следовательно, наше исследование разбивается еще на два случая.

Случай 1: $U = \{\overline{1}\}$. Пусть $\overline{1}$ – единственный обратимый элемент в $R/2R$, который поднимается по модулю $2R$. Тогда определение эквивалентности векторов $z = (z_1, \ldots, z_k)$, $h = (h_1, \ldots, h_k) \in (R/2R)^k$ можно записать в виде

$$z \sim_{even,U} h \Leftrightarrow \exists\ c_{ij} \in R/2R : h_i = z_i + \sum_{j=1}^{i-1} c_{ij}^2 z_j.$$

Очевидно, что при такой формулировке нулевой вектор θ эквивалентен только себе.

Лемма 5. *Пусть* $a = (a_1, \ldots, a_k), b = (b_1, \ldots, b_k) \in (R/2R)^k$ *– ненулевые. Если* $a \sim_{even,U} b$, *то* $\exists\ s, 1 \leqslant s \leqslant k\ a_s = b_s \neq \overline{0}\ u\ \forall\ i < s\ a_i = b_i = \overline{0}$.

Доказательство. Так как $a \neq \theta$ и $b \neq \theta$, следовательно существует минимальный индекс $1 \leqslant m \leqslant k$ такой, что $a_m \neq \overline{0}$ и существует минимальный индекс $1 \leqslant n \leqslant k$ такой, что $b_n \neq \overline{0}$. Докажем, что $m = n$.

Допустим $m < n$. Тогда так как $a \sim_{even,U} b$, то

$$a_m = b_m + \sum_{j=1}^{m-1} c_{mj}^2 b_j = \overline{0} + \sum_{j=1}^{m-1} c_{mj}^2 \cdot \overline{0}.$$

Значит, $a_m = \overline{0}$. Противоречие.

Заметим, что если $m = s = n$, то $a_s = b_s + \sum\limits_{j=1}^{s-1} c_{sj}^2 b_j = b_s$. $\square$

Для каждого s от 1 до k положим

$$z_s = (\overline{z_1}, \ldots, \overline{z_s}, \ldots, \overline{z_k}) \in (R/2R)^k,$$

где $\overline{z_s} \neq \overline{0}$, а все остальные элементы равны $\overline{0}$. По лемме 5 $z_s \not\sim_{even,U} z_{s_1}$ если $s \neq s_1$ или $\overline{z_s} \neq \overline{z_{s_1}}$.

Предложение 3. *Пусть* $a = (a_1, \ldots, a_s, \ldots, a_k) \in (R/2R)^k$. *Тогда* $a \sim_{even,U} z_s \Leftrightarrow$ $\forall\ 1 \leqslant i < s\ a_i = \overline{0}, a_s = \overline{z_s}\ u\ \forall\ s < f \leqslant k\ a_f \in \{\overline{0}, \overline{z_s}\}$.

Доказательство. ($\Leftarrow$) Так как $\overline{z_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0} = \overline{z_i} + \sum_{j=1}^{i-1} c_{ij}^2 \overline{z_j},$$

для любых $c_{ij} \in R/2R$. Выберем произвольный элемент a_f, где $s < f \leqslant k$ и покажем, что будет выполняться равенство

$$a_f = \overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{z_j},$$

для некоторых $c_{fj} \in R/2R$. Очевидно, что всегда можно выбрать элемент $c_{fs} \in R/2R$ так, чтобы выполнялось равенство $a_f = c_{fs}^2 \overline{z_s}$. Осталось заметить, что

$$a_f = c_{fs}^2 \overline{z_s} = \overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{z_j},$$

где $c_{fj} = \overline{0}$ при $j \neq s$.

Для индекса s, имеем

$$a_s = \overline{z_s} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j},$$

для любых $c_{sj} \in R/2R$.

($\Rightarrow$) Пусть теперь $a \sim_{even,U} z_s$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j}.$$

Причем, если $l < s$ имеем

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j} = \overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0} = \overline{0}.$$

Если $l = s$, тогда

$$a_s = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0} = \overline{z_s}.$$

Если же $l > s$, тогда

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j} = \overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j} = c_{ls}^2 \overline{z_s}.$$

По лемме 1 $c_{ls}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $c_{ls}^2 \overline{z_s} \in \{\overline{0}, \overline{z_s}\}$. $\square$

Для каждой пары s, t различных натуральных чисел от 1 до k положим

$$z_{st} = (\overline{z_1}, \ldots, \overline{z_s}, \ldots, \overline{z_t}, \ldots, \overline{z_k}) \in (R/2R)^k,$$

где $\overline{z_s} = \overline{1}, \overline{z_t} \in \{\overline{\varphi}, \overline{\varphi+1}\}$ или $\overline{z_s} = \overline{\varphi}, \overline{z_t} \in \{\overline{1}, \overline{\varphi+1}\}$, или $\overline{z_s} = \overline{\varphi+1}, \overline{z_t} \in \{\overline{1}, \overline{\varphi}\}$, а все остальные элементы равны $\overline{0}$.

Из Леммы 5 следует, что $z_{st} \not\sim_{even,U} z_{s_1 t_1}$, если $s \neq s_1$ или $\overline{z_s} \neq \overline{z_{s_1}}$, а из Предложения 3, что $z_{st} \not\sim_{even,U} z_s$.

Предложение 4. *Пусть* $a = (a_1, \ldots, a_s, \ldots, a_t, \ldots, a_k) \in (R/2R)^k$. *Тогда* $a \sim_{even,U} z_{st} \Leftrightarrow \forall\ 1 \leqslant i < s\ a_i = \overline{0}, a_s = \overline{z_s}, \forall\ s < f < t\ a_f \in \{\overline{0}, \overline{z_s}\}$ *и* $a_t \in \{\overline{z_t}, \overline{z_t} + \overline{z_s}\}$.

Доказательство. ($\Leftarrow$) Так как $\overline{z_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0} = \overline{z_i} + \sum_{j=1}^{i-1} c_{ij}^2 \overline{z_j},$$

для любых $c_{ij} \in R/2R$.

Для индекса s, имеем

$$a_s = \overline{z_s} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j},$$

для любых $c_{sj} \in R/2R$.

Для индекса $s < f < t$ всегда можно выбрать элемент $c_{fs} \in R/2R$ так, чтобы выполнялось равенство $a_f = c_{fs}^2 \overline{z_s}$. Осталось заметить, что

$$a_f = c_{fs}^2 \overline{z_s} = \overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{z_j},$$

где $c_{fj} = \overline{0}$ при $j \neq s$.

Выберем произвольный элемент a_m, где $t < m \leqslant k$ и покажем, что будет выполняться равенство

$$a_m = \overline{z_m} + \sum_{j=1}^{m-1} c_{mj}^2 \overline{z_j},$$

для некоторых $c_{mj} \in R/2R$. Действительно, выберем $c_{ms}, c_{mt} \in R/2R$ так, чтобы выполнялось равенство $a_m = c_{ms}^2\overline{z_s} + c_{mt}^2\overline{z_t}$. Несложно убедиться, что такие элементы существуют для любого значения a_m. Теперь заметим, что

$$a_m = c_{ms}^2\overline{z_s} + c_{mt}^2\overline{z_t} = \overline{z_m} + \sum_{j=1}^{m-1} c_{mj}^2\overline{z_j},$$

где $c_{mj} = \overline{0}$ при $j \neq s$ и $j \neq t$.

Для индекса t, выбрав $c_{ts} \in R/2R$ так, чтобы $a_t = \overline{z_t} + c_{ts}^2\overline{z_s}$, имеем

$$a_t = \overline{z_t} + c_{ts}^2\overline{z_s} = \overline{z_t} + \sum_{j=1}^{t-1} c_{tj}^2\overline{z_j},$$

где $c_{tj} = \overline{0}$ при $j \neq s$.

($\Rightarrow$) Пусть теперь $a \sim_{even,U} z_{st}$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j}.$$

Причем, если $l < s$ имеем

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j} = \overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0} = \overline{0}.$$

Если $l = s$, тогда

$$a_s = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2\overline{z_j} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0} = \overline{z_s}.$$

Если $s < l < t$, тогда

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j} = \overline{0} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j} = c_{ls}^2\overline{z_s}.$$

По лемме 1 $c_{ls}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $c_{ls}^2\overline{z_s} \in \{\overline{0}, \overline{z_s}\}$.

Если же $l = t$, то

$$a_t = \overline{z_t} + \sum_{j=1}^{t-1} c_{tj}^2\overline{z_j} = \overline{z_t} + c_{ts}^2\overline{z_s}.$$

По лемме 1 $c_{ts}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $\overline{z_t} + c_{ts}^2\overline{z_s} \in \{\overline{z_t}, \overline{z_t} + \overline{z_s}\}$. $\square$

Таким образом, из Предложений 3 и 4 следует, что любой ненулевой вектор в $(R/2R)^k$ эквивалентен z_s или z_{st}. Прямой подсчет показывает, что векторов типа z_s – $3k$ вариантов, типа z_{st} – $3k^2 - 3k$ вариантов и один нулевой вектор. Следовательно, $|(R/2R)^k/\sim_{even,U}| = 3k^2 + 1$. А тогда в силу Теоремы 4 и Следствия 1 [3] имеем $|\beta| = 3k^2 + 2$, где β – множество классов эквивалентности инволюций в $T_{2k}(\mathbb{Z}[\sqrt{d}])$. Заметим, что формула верна и при $k = 1$.

Случай 2: $U = \{\overline{1}, \overline{\varphi}\}$. Пусть теперь все обратимые элементы в $R/2R$ поднимаются по модулю $2R$. Тогда определение эквивалентности векторов $z = (z_1, \ldots, z_k)$, $h = (h_1, \ldots, h_k) \in (R/2R)^k$ будет записано в следующем виде:

$$z \sim_{even,U} h \Leftrightarrow \exists\ \lambda \in U\ \exists\ c_{ij} \in R/2R : h_i = \lambda(z_i + \sum_{j=1}^{i-1} c_{ij}^2 z_j).$$

При такой формулировке нулевой вектор θ по прежнему эквивалентен только себе. Заметим, что если $\lambda \in U$, то $\lambda \cdot \overline{\varphi + 1} = \overline{\varphi + 1}$.

Лемма 6. *Пусть* $a = (a_1, \ldots, a_k), b = (b_1, \ldots, b_k) \in (R/2R)^k$ *– ненулевые. Если* $a \sim_{even,U} b$, *то* $\exists\ s, 1 \leqslant s \leqslant k\ a_s = b_s = \overline{\varphi + 1}$ *или* $a_s, b_s \in \{\overline{1}, \overline{\varphi}\}\ u\ \forall\ i < s\ a_i = b_i = \overline{0}$.

Доказательство. Доказательство данного утверждения аналогично доказательству Леммы 5. □

Для каждого s от 1 до k положим

$$z_s = (\overline{z_1}, \ldots, \overline{z_s}, \ldots, \overline{z_k}) \in (R/2R)^k,$$

где $\overline{z_s} = \overline{\varphi + 1}$, а все остальные элементы равны $\overline{0}$, и

$$h_s = (\overline{h_1}, \ldots, \overline{h_s}, \ldots, \overline{h_k}) \in (R/2R)^k,$$

где $\overline{h_s} = \overline{1}$, а все остальные элементы равны $\overline{0}$.

Из Леммы 6 следует, что $z_s \not\sim_{even,U} h_s$ и $z_s \not\sim_{even,U} z_{s_1}, h_s \not\sim_{even,U} h_{s_1}$, если $s \neq s_1$. Также очевидно, что $h_s \sim_{even,U} h'_s$, где

$$h'_s = (\overline{0}, \ldots, \overline{0}, \overline{h'_s}, \overline{0}, \ldots, \overline{0}) \in (R/2R)^k, \overline{h'_s} = \overline{\varphi}.$$

Предложение 5. *Пусть* $a = (a_1, \ldots, a_s, \ldots, a_k) \in (R/2R)^k$. *Тогда*

1. $a \sim_{even,U} z_s \Leftrightarrow$
   $\forall\ 1 \leqslant i < s\ a_i = \overline{0}, a_s = \overline{\varphi + 1}\ u\ \forall\ s < f \leqslant k\ a_f \in \{\overline{0}, \overline{\varphi + 1}\}$;
2. $a \sim_{even,U} h_s \Leftrightarrow$
   $\forall\ 1 \leqslant i < s\ a_i = \overline{0}, a_s \in U\ u\ \forall\ s < f \leqslant k\ a_f \in \{\overline{0}, a_s\}$.

Доказательство.

1. ($\Leftarrow$) Положим $\lambda = \overline{1}$. Так как $\overline{z_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \lambda(\overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0}) = \lambda(\overline{z_i} + \sum_{j=1}^{i-1} c_{ij}^2 \overline{z_j}),$$

для любых $c_{ij} \in R/2R$. Выберем произвольный элемент a_f, где $s < f \leqslant k$, и покажем, что будет выполняться равенство

$$a_f = \lambda(\overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{z_j}),$$

для некоторых $c_{fj} \in R/2R$. Очевидно, что всегда можно выбрать элемент $c_{fs} \in R/2R$ так, чтобы выполнялось равенство $a_f = c_{fs}^2 \overline{\varphi + 1}$. Осталось заметить, что

$$a_f = c_{fs}^2 \overline{\varphi + 1} = c_{fs}^2 \lambda \overline{\varphi + 1} = \lambda c_{fs}^2 \overline{\varphi + 1} =$$

$$= \lambda c_{fs}^2 \overline{z_s} = \lambda(\overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{z_j}),$$

где $c_{fj} = \overline{0}$ при $j \neq s$. Для индекса s, имеем

$$a_s = \overline{\varphi + 1} = \lambda \overline{z_s} = \lambda(\overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j}),$$

для любых $c_{sj} \in R/2R$. ($\Rightarrow$) Пусть теперь $a \sim_{even,U} z_s$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \lambda(\overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j}).$$

Причем, если $l < s$ имеем

$$a_l = \lambda(\overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0}) = \overline{0}.$$

Если $l = s$, тогда

$$a_s = \lambda(\overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j}) = \lambda(\overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0}) = \lambda \overline{z_s} = \overline{\varphi + 1}.$$

Если же $l > s$, тогда

$$a_l = \lambda(\overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j}) = \lambda c_{ls}^2 \overline{z_s} = c_{ls}^2 \lambda \overline{z_s} = c_{ls}^2 \overline{\varphi + 1}.$$

По лемме 1 $c_{ls}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $c_{ls}^2 \overline{\varphi + 1} \in \{\overline{0}, \overline{\varphi + 1}\}$;

2. ($\Leftarrow$) Положим $\lambda = a_s$. Так как $\overline{h_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \lambda(\overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0}) = \lambda(\overline{h_i} + \sum_{j=1}^{i-1} c_{ij}^2 \overline{h_j}),$$

для любых $c_{ij} \in R/2R$. Выберем произвольный элемент a_f, где $s < f \leqslant k$ и покажем, что будет выполняться равенство

$$a_f = \lambda(\overline{h_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{h_j}),$$

для некоторых $c_{fj} \in R/2R$. Очевидно, что всегда можно выбрать элемент $c_{fs} \in R/2R$ так, чтобы выполнялось равенство $a_f = \lambda c_{fs}^2$. Осталось заметить, что

$$a_f = \lambda c_{fs}^2 = \lambda c_{fs}^2 \overline{h_s} = \lambda(\overline{h_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{h_j}),$$

где $c_{fj} = \overline{0}$ при $j \neq s$. Для индекса s, имеем

$$a_s = \lambda = \lambda \overline{h_s} = \lambda(\overline{h_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{h_j}),$$

для любых $c_{sj} \in R/2R$. ($\Rightarrow$) Пусть теперь $a \sim_{even,U} h_s$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \lambda(\overline{h_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}).$$

Причем, если $l < s$ имеем

$$a_l = \lambda(\overline{h_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0}) = \overline{0}.$$

Если $l = s$, тогда

$$a_s = \lambda(\overline{h_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{h_j}) = \lambda(\overline{h_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0}) = \lambda\overline{h_s} = \lambda.$$

Если же $l > s$, тогда

$$a_l = \lambda(\overline{h_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}) = \lambda c_{ls}^2 \overline{h_s} = \lambda c_{ls}^2.$$

По лемме 1 $c_{ls}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $\lambda c_{ls}^2 \in \{\overline{0}, \lambda\}$.

□

Для каждой пары s, t различных натуральных чисел от 1 до k положим

$$z_{st} = (\overline{z_1}, \ldots, \overline{z_s}, \ldots, \overline{z_t}, \ldots, \overline{z_k}) \in (R/2R)^k,$$

где $\overline{z_s} = \overline{\varphi + 1}, \overline{z_t} = \overline{1}$, а все остальные элементы равны $\overline{0}$, и

$$h_{st} = (\overline{h_1}, \ldots, \overline{h_s}, \ldots, \overline{h_t}, \ldots, \overline{h_k}) \in (R/2R)^k,$$

где $\overline{h_s} = \overline{1}, \overline{h_t} = \overline{\varphi}$, а все остальные элементы равны $\overline{0}$.

Из Леммы 6 следует, что $z_{st} \not\sim_{even,U} h_{st}$ и $z_{st} \not\sim_{even,U} z_{s_1t_1}, h_{st} \not\sim_{even,U} h_{s_1t_1}$, если $s \neq s_1$, а из Предложения 5 следует, что $z_{st} \not\sim_{even,U} z_s, z_{st} \not\sim_{even,U} h_s$ и $h_{st} \not\sim_{even,U} z_s, h_{st} \not\sim_{even,U} h_s$.

Предложение 6. *Пусть* $a = (a_1, \ldots, a_s, \ldots, a_t, \ldots, a_k) \in (R/2R)^k$. *Тогда*

1. $a \sim_{even,U} z_{st} \Leftrightarrow$
$\forall\ 1 \leqslant i < s\ a_i = \overline{0}, a_s = \overline{\varphi + 1}\ u\ \forall\ s < f < t\ a_f \in \{\overline{0}, \overline{\varphi + 1}\},\ u\ a_t \in \{\overline{1}, \overline{\varphi}\}$;

2. $a \sim_{even,U} h_{st} \Leftrightarrow$
$\forall\ 1 \leqslant i < s\ a_i = \overline{0}, a_s \in U\ u\ \forall\ s < f < t\ a_f \in \{\overline{0}, a_s\},\ u\ a_t \in \{a_s \cdot \overline{\varphi}, \overline{\varphi + 1}\}$.

Доказательство.

1. ($\Leftarrow$) Положим $\lambda = \overline{1}$. Так как $\overline{z_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \lambda(\overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0}) = \lambda(\overline{z_i} + \sum_{j=1}^{i-1} c_{ij}^2 \overline{z_j}),$$

для любых $c_{ij} \in R/2R$. Выберем произвольный элемент a_f, где $s < f < t$, и покажем, что будет выполняться равенство

$$a_f = \lambda(\overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2 \overline{z_j}),$$

для некоторых $c_{fj} \in R/2R$. Очевидно, что всегда можно выбрать элемент $c_{fs} \in R/2R$ так, чтобы выполнялось равенство $a_f = c_{fs}^2\overline{\varphi+1}$. Осталось заметить, что

$$a_f = c_{fs}^2\overline{\varphi+1} = c_{fs}^2\lambda\overline{\varphi+1} = \lambda c_{fs}^2\overline{\varphi+1} =$$

$$= \lambda c_{fs}^2\overline{z_s} = \lambda(\overline{z_f} + \sum_{j=1}^{f-1} c_{fj}^2\overline{z_j}),$$

где $c_{fj} = \overline{0}$ при $j \neq s$.

Выберем произвольный элемент a_m, где $t < m \leqslant k$ и покажем, что будет выполняться равенство

$$a_m = \lambda(\overline{z_m} + \sum_{j=1}^{m-1} c_{mj}^2\overline{z_j}),$$

для некоторых $c_{mj} \in R/2R$. Действительно, выберем $c_{ms}, c_{mt} \in R/2R$ так, чтобы выполнялось равенство $a_m = c_{ms}^2\overline{\varphi+1} + \lambda c_{mt}^2$. Несложно убедиться, что такие элементы существуют для любого значения a_m. Теперь заметим, что

$$a_m = c_{ms}^2\overline{\varphi+1} + \lambda c_{mt}^2 = c_{ms}^2\lambda\overline{\varphi+1} + \lambda c_{mt}^2\overline{z_t} = \lambda(c_{ms}^2\overline{z_s} + c_{mt}^2\overline{z_t}) = \lambda(\overline{z_m} + \sum_{j=1}^{m-1} c_{mj}^2\overline{z_j}),$$

где $c_{mj} = \overline{0}$ при $j \neq s$ и $j \neq t$.

Для индекса t, выбрав $c_{ts} \in R/2R$ так, чтобы $a_t = \lambda + c_{ts}^2\overline{\varphi+1}$, имеем

$$a_t = \lambda + c_{ts}^2\overline{\varphi+1} = \lambda\overline{z_t} + c_{ts}^2\lambda\overline{\varphi+1} = \lambda(\overline{z_t} + c_{ts}^2\overline{z_s}) = \lambda(\overline{z_t} + \sum_{j=1}^{t-1} c_{tj}^2\overline{z_j}),$$

где $c_{tj} = \overline{0}$ при $j \neq s$.

($\Rightarrow$) Пусть теперь $a \sim_{even,U} z_{st}$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \lambda(\overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j}).$$

Причем, если $l < s$ имеем

$$a_l = \lambda(\overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0}) = \overline{0}.$$

Если $l = s$, тогда

$$a_s = \lambda(\overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2\overline{z_j}) = \lambda(\overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0}) = \lambda\overline{z_s} = \overline{\varphi+1}.$$

Если $s < l < t$, тогда

$$a_l = \lambda(\overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2\overline{z_j}) = \lambda c_{ls}^2\overline{z_s} = c_{ls}^2\lambda\overline{z_s} = c_{ls}^2\overline{\varphi+1}.$$

По лемме 1 $c_{ls}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $c_{ls}^2\overline{\varphi+1} \in \{\overline{0}, \overline{\varphi+1}\}$.

Если же $l = t$, тогда

$$a_t = \lambda(\overline{z_t} + \sum_{j=1}^{t-1} c_{tj}^2\overline{z_j}) = \lambda(\overline{z_t} + c_{ts}^2\overline{z_s}) = \lambda + c_{ts}^2\overline{\varphi+1}.$$

По лемме 1 $c_{ts}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $\lambda + c_{ts}^2\overline{\varphi+1} \in \{\overline{1}, \overline{\varphi}\}$;

2. ($\Leftarrow$) Положим $\lambda = a_s$. Так как $\overline{h_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \lambda(\overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0}) = \lambda(\overline{h_i} + \sum_{j=1}^{i-1} c_{ij}^2\overline{h_j}),$$

для любых $c_{ij} \in R/2R$.

Выберем произвольный элемент a_f, где $s < f < t$ и покажем, что будет выполняться равенство

$$a_f = \lambda(\overline{h_f} + \sum_{j=1}^{f-1} c_{fj}^2\overline{h_j}),$$

для некоторых $c_{fj} \in R/2R$. Очевидно, что всегда можно выбрать элемент $c_{fs} \in R/2R$ так, чтобы выполнялось равенство $a_f = \lambda c_{fs}^2$. Осталось заметить, что

$$a_f = \lambda c_{fs}^2 = \lambda c_{fs}^2\overline{h_s} = \lambda(\overline{h_f} + \sum_{j=1}^{f-1} c_{fj}^2\overline{h_j}),$$

где $c_{fj} = \overline{0}$ при $j \neq s$. Для индекса s, имеем

$$a_s = \lambda = \lambda\overline{h_s} = \lambda(\overline{h_s} + \sum_{j=1}^{s-1} c_{sj}^2\overline{h_j}),$$

для любых $c_{sj} \in R/2R$.

Выберем произвольный элемент a_m, где $t < m \leqslant k$ и покажем, что будет выполняться равенство

$$a_m = \lambda(\overline{h_m} + \sum_{j=1}^{m-1} c_{mj}^2\overline{h_j}),$$

для некоторых $c_{mj} \in R/2R$. Действительно, выберем $c_{ms}, c_{mt} \in R/2R$ так, чтобы выполнялось равенство положим $a_m = \lambda(c_{ms}^2 + c_{mt}^2\overline{\varphi})$. Несложно убедиться, что такие элементы существуют для любого значения a_m. Теперь заметим, что

$$a_m = \lambda(c_{ms}^2 + c_{mt}^2\overline{\varphi}) = \lambda(c_{ms}^2\overline{h_s} + c_{mt}^2\overline{h_t}) = \lambda(\overline{h_m} + \sum_{j=1}^{m-1} c_{mj}^2\overline{h_j}),$$

где $c_{mj} = \overline{0}$ при $j \neq s$ и $j \neq t$.

Для индекса t, выбрав $c_{ts} \in R/2R$ так, чтобы $a_t = \lambda(\overline{\varphi} + c_{ts}^2)$, имеем

$$a_t = \lambda(\overline{\varphi} + c_{ts}^2) = \lambda(\overline{h_t} + c_{ts}^2\overline{h_s}) = \lambda(\overline{h_t} + \sum_{j=1}^{t-1} c_{tj}^2\overline{h_j}),$$

где $c_{tj} = \overline{0}$ при $j \neq s$. ($\Rightarrow$) Пусть теперь $a \sim_{even,U} h_{st}$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \lambda(\overline{h_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}).$$

Причем, если $l < s$ имеем

$$a_l = \lambda(\overline{h_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0}) = \overline{0}.$$

Если $l = s$, тогда

$$a_s = \lambda(\overline{h_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{h_j}) = \lambda(\overline{h_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0}) = \lambda\overline{h_s} = \lambda.$$

Если $s < l < t$, тогда

$$a_l = \lambda(\overline{h_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}) = \lambda(\overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{h_j}) = \lambda c_{ls}^2 \overline{h_s} = \lambda c_{ls}^2.$$

По Лемме 1 $c_{ls}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $\lambda c_{ls}^2 \in \{\overline{0}, \lambda\}$.

Если же $l = t$, тогда

$$a_t = \lambda(\overline{h_t} + \sum_{j=1}^{t-1} c_{tj}^2 \overline{h_j}) = \lambda(\overline{h_t} + c_{ts}^2 \overline{h_s}) = \lambda(\overline{\varphi} + c_{ts}^2).$$

По Лемме 1 $c_{ts}^2 \in \{\overline{0}, \overline{1}\}$, следовательно $\lambda(\overline{\varphi} + c_{ts}^2) \in \{\lambda \cdot \overline{\varphi}, \overline{\varphi + 1}\}$.

□

Следствие 1. *Пусть*

$$z'_{st} = (\overline{0}, \ldots, \overline{0}, \overline{z'_s}, \overline{0}, \ldots, \overline{0}, \overline{z'_t}, \overline{0}, \ldots, \overline{0}) \in (R/2R)^k,$$

где $\overline{z'_s} = \overline{\varphi + 1}, \overline{z'_t} = \overline{\varphi}$, *и*

$$h'_{st} = (\overline{0}, \ldots, \overline{0}, \overline{h'_s}, \overline{0}, \ldots, \overline{0}, \overline{h'_t}, \overline{0}, \ldots, \overline{0}) \in (R/2R)^k,$$

где $\overline{h'_s} = \overline{\varphi}, \overline{h'_t} = \overline{1}$ *или* $\overline{h'_s} = \overline{1}, \overline{h'_t} = \overline{\varphi + 1}$, *или* $\overline{h'_s} = \overline{\varphi}, \overline{h'_t} = \overline{\varphi + 1}$. *Тогда* $z_{st} \sim_{even,U} z'_{st}$ *и* $h_{st} \sim_{even,U} h'_{st}$.

Таким образом, из Предложений 5 и 6 и Следствия 1 следует, что любой ненулевой вектор в $(R/2R)^k$ эквивалентен одному из векторов z_s, h_s, z_{st}, h_{st}. Прямой подсчет показывает, что векторов типа z_s и h_s – $2k$ вариантов, типа z_{st} и h_{st} – $k^2 - k$ вариантов и один нулевой вектор. Следовательно, $|(R/2R)^k/\sim_{even,U}| = k^2 + k + 1$. И тогда в силу Теоремы 4 и Следствия 1 [3] имеем $|\beta| = k^2 + k + 2$, где β – множество классов эквивалентности инволюций в $T_{2k}(\mathbb{Z}[\sqrt{d}])$. Таким образом, нами доказана **Теорема 1**.

Далее везде $d \equiv 2(\mathrm{mod}4)$.

Так как $d \equiv 2(\mathrm{mod}4)$, то в $R/2R$ обратимыми элементами являются $\overline{1}$ и $\overline{\varphi + 1}$.

Лемма 7. *Пусть $d \equiv 2(\mathrm{mod}4)$. Тогда все обратимые элементы в $R/2R$ поднимаются по модулю $2R$ тогда и только тогда, когда разрешимо в целых числах уравнение*

$$x^2 - dy^2 = -1, \text{ где } x, y - \text{ нечетные.} \quad (**)$$

Причем, если указанное уравнение не обладает требуемыми решениями, то $U = \{\overline{1}\}$.

Доказательство. Как уже было отмечено выше, $\overline{1}$ является обратимым элементом, который всегда поднимается по модулю $2R$. Пусть теперь $\overline{\varphi+1}$ поднимается по модулю $2R$. Элемент $a + b\sqrt{d}$ кольца R принадлежит смежному классу $\overline{\varphi+1}$ тогда и только тогда, когда a и b — нечетные. Такой элемент будет обратим в кольце R тогда и только тогда, когда разрешимо в целых числах уравнение

$$x^2 - dy^2 = \pm 1, \text{ где } x, y - \text{ нечетные.}$$

В этом уравнении перейдем к сравнению по модулю 4. Получим

$$1 - 2 \cdot 1 \equiv \pm 1(\mathrm{mod}4).$$

Теперь становится очевидным, что уравнение вида $x^2 - dy^2 = 1$ не имеет решений при нечетных x, y. К тому же убеждаемся в том, что любое решение уравнения $x^2 - dy^2 = -1$ имеет нечетные x, y. Второе утверждение леммы очевидно. □

Как и в предыдущем случае разрешимость уравнения (**) зависит от конкретного значения d. Общих результатов, описывающих разрешимость уравнения (**) в терминах d, на данный момент также получено не было. Все же мы можем получить формулу для нахождения некоторых d, при которых уравнение (**) разрешимо. Возьмём $y = 1, x = 2n+1, n \in \mathbb{N} \cup \{0\}$ и подставим в уравнение (**). Выразив d, получим

$$d = (2n+1)^2 + 1 = 4n^2 + 4n + 2.$$

Заметим, что если $n = 3$, то $d = 50 = 5^2 \cdot 2$. Но d должно быть бесквадратным числом. Однако мы легко можем обойти это затруднение. Числа, полученные при помощи формулы $4n^2 + 4n + 2$, не делятся на 4, следовательно, не могут содержать в себе квадрата четного числа. Если же d будет содержать квадрат нечетного числа, то $d = d_1 m^2$, где m – нечетно, а $d_1 \equiv 2(\mathrm{mod}4)$ и d_1 – бесквадратное число. Пусть (x_0, y_0) – решение уравнения (**), тогда (x_0, my_0) – решение $x^2 - d_1 y^2 = -1$.

Приведем примеры некоторых значений d, при которых уравнение (**) разрешимо

$$d = 2, 10, 26, 58, 74, 82, \ldots.$$

Переходя к сравнению по модулю 8 в уравнениях $x^2 - 6y^2 = -1$ или $x^2 - 14y^2 = -1$ несложно проверить, что, например, при $d = 6, 14$ уравнение (**) не разрешимо.

Таким образом, в зависимости от конкретного d в $R/2R$ снова могут встречаться обратимые элементы, которые поднимаются по модулю $2R$ или которые не поднимаются по модулю $2R$.

В силу того, что $R/2R \cong \mathbb{Z}_2[x]/(x^2)$ (см. Лемму 1), все утверждения, доказанные в предыдущем параграфе, будут выполняться и в случае, когда $d \equiv 2(\mathrm{mod}4)$ с точностью до замены $\overline{\varphi}$ на $\overline{\varphi+1}$ и $\overline{\varphi+1}$ на $\overline{\varphi}$. Таким образом, если $U = \{\overline{1}\}$, то $|\beta| = 3k^2 + 2$, если же $U = \{\overline{1}, \overline{\varphi+1}\}$, то
$|\beta| = k^2 + k + 2$. Теперь мы доказали **Теорему 2**.

4. Классификация инволюций при $d \equiv 1(\mathrm{mod}4)$

Пусть теперь $d \equiv 1(\mathrm{mod}4)$ – бесквадратное целое и $R = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Здесь и далее через φ будем обозначать $\varphi = \frac{1+\sqrt{d}}{2} \in R$.

Так как $d \equiv 1(\mathrm{mod}4)$, то $d = 4t+1, t \in \mathbb{Z}$. Рассмотрим, чему равен квадрат элемента $\overline{\varphi} \in R/2R$.

$$\overline{\varphi}^2 = \overline{\frac{1+2\sqrt{d}+d}{4}} = \overline{\frac{2+2\sqrt{d}+4t}{4}} = \overline{t+\frac{1+\sqrt{d}}{2}} = \overline{t+\varphi} = \begin{cases} \overline{\varphi}, \text{ если } t - \text{ четное;} \\ \overline{\varphi+1}, \text{ если } t - \text{ нечетное.} \end{cases}$$

И снова наше исследование распадается на случаи.

Случай 1: t – четное.

Лемма 8. *Пусть t – четное. Тогда $R/2R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Доказательство. Если t – четное, тогда $\overline{\varphi}^2 = \overline{\varphi}$ и $\overline{\varphi+1}^2 = \overline{\varphi^2+2\varphi+1} = \overline{3\varphi+1} = \overline{\varphi+1}$. Следовательно, $R/2R$ – булево, а значит $R/2R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □ Так как $\overline{\varphi} \cdot \overline{\varphi+1} = \overline{\varphi^2+\varphi} = \overline{0}$, то $\overline{1}$ – единственный обратимый элемент кольца $R/2R$.

Таким образом, из Теоремы 6 [3] следует, что в $T_{2k+1}(\mathbb{Z}[\varphi])$ все инволюции попарно эквивалентны, а в $T_{2k}(\mathbb{Z}[\varphi])$ ровно $(k+1)^2$ классов эквивалентности инволюций.

Случай 2: t – нечетное.

Лемма 9. *Пусть t – нечетное. Тогда $R/2R = \mathbb{F}_4$.*

Доказательство. Если t – нечетное, то

$$\overline{\varphi} \cdot \overline{\varphi+1} = \overline{\varphi^2+\varphi} = \overline{\varphi+1+\varphi} = \overline{1},$$

значит $\overline{\varphi}$ и $\overline{\varphi+1}$ взаимнообратные. Следовательно, $R/2R$ – поле $\mathbb{F}_4$. □

Для дальнейших рассуждений нам потребуется ввести норму в R. Для этого перейдем к видоизмененной формулировке устройства кольца R.

$$a + b\varphi = a + b\frac{1+\sqrt{d}}{2} = \frac{2a+b+b\sqrt{d}}{2} = \frac{2a+b}{2} + \frac{b\sqrt{d}}{2}$$

Сделаем замену $r = 2a+b, s = b$. Заметим, что $(r-s) \vdots 2$, тогда

$$\mathbb{Z}[\varphi] = R = \left\{ \frac{r}{2} + \frac{s}{2}\sqrt{d} \mid r, s \in \mathbb{Z} \text{ и } (r-s) \vdots 2 \right\}.$$

Элемент кольца R обратим тогда и только тогда, когда его норма $\left|\frac{r}{2} + \frac{s}{2}\sqrt{d}\right| = \frac{r^2 - s^2 d}{4} = \pm 1$ или $r^2 - s^2 d = \pm 4$.

Лемма 10. *Пусть $d \equiv 1(\mathrm{mod}4)$. Тогда все обратимые элементы в $R/2R$ поднимаются по модулю $2R$ тогда и только тогда, когда разрешимо в целых числах уравнение*

$$x^2 - dy^2 = \pm 4, \text{ где } x, y - \text{ нечетные одновременно.} \quad (***)$$

Причем, если указанное уравнение не обладает требуемыми решениями, то $U = \{\overline{1}\}$.

Доказательство.

Как уже было отмечено выше, $\overline{1}$ является обратимым элементом, который всегда поднимается по модулю $2R$. Пусть теперь $\overline{\varphi}$ и $\overline{\varphi+1}$ поднимаются по модулю $2R$. Так как U – подгруппа $(R/2R)^*$ (группы обратимых элементов $R/2R$), то либо $U=\{\overline{1}\}$, либо $U=\{\overline{1},\overline{\varphi},\overline{\varphi+1}\}$.

Далее, элемент $a+b\dfrac{1+\sqrt{d}}{2}$ кольца R принадлежит смежному классу $\overline{\varphi}$ тогда и только тогда, когда a четное, а b нечетное. Следовательно, $r=2a+b$ и $s=b$ одновременно нечетные. Или же элемент $a+b\dfrac{1+\sqrt{d}}{2}$ кольца R принадлежит смежному классу $\overline{\varphi+1}$ тогда и только тогда, когда a и b нечетные. Следовательно, r и s снова одновременно нечетные. При этом, элемент $a+b\dfrac{1+\sqrt{d}}{2}$ будет обратим в кольце R тогда и только тогда, когда разрешимо в целых числах уравнение

$$x^2-dy^2=\pm 4,\ \text{где } x,y- \text{ нечетные одновременно.}$$

Рассматривая уравнение $x^2-dy^2=\pm 4$ по модулю 4, несложно проверить, что значения x и y либо оба четные, либо оба нечетные.

Заметим, что если r и s – четные, то b – четное, a – четное или нечетное. Значит, если уравнение $x^2-dy^2=\pm 4$ имеет только четные решения, то соответствующие обратимые элементы $a+b\varphi$ кольца R попадут в класс $\overline{1}$. Второе утверждение леммы очевидно. $\square$

Следующее утверждение дает критерий разрешимости уравнения (***).

Лемма 11. *Уравнение (***) разрешимо тогда и только тогда, когда наименьшее положительное решение уравнения $x^2-dy^2=4$ нечетно.*

Доказательство. Достаточность условия очевидна. Докажем его необходимость. Предположим, что наименьшее положительное решение уравнения $x^2-dy^2=4$ четно. Сокращая обе части уравнения на 4, убеждаемся в том, что это решение есть $(2x_*,2y_*)$, где (x_*,y_*) – наименьшее положительное решение уравнения $x^2-dy^2=1$. Пользуясь Леммой 6 [5] и Теоремой 3 [5], получаем, что $(2x_*,2y_*)$ – единственное базовое решение уравнения $x^2-dy^2=4$, и все его положительные решения имеют вид

$$x_n+y_n\sqrt{d}=(2x_*+2y_*\sqrt{d})(x_*+y_*\sqrt{d})^{n-1}=2(x_*+y_*\sqrt{d})^n,$$

где n – натуральное число. Таким образом, уравнение $x^2-dy^2=4$ имеет только четные решения.

Поскольку уравнение (***) разрешимо, то существует нечетное решение уравнения $x^2-dy^2=-4$. Обозначим это решение через (x_0,y_0). Рассмотрим следующее равенство

$$(x_0+y_0\sqrt{d})^2=x_0^2+dy_0^2+2x_0y_0\sqrt{d}=X+Y\sqrt{d},$$

где $X=x_0^2+dy_0^2, Y=2x_0y_0$. Несложно заметить, что пара (X,Y) является решением уравнения $x^2-dy^2=16$. Действительно, имеем

$$(x_0-y_0\sqrt{d})^2=X-Y\sqrt{d},$$

откуда, перемножая последние равенства, получим

$$(x_0^2-dy_0^2)^2=(-4)^2=X^2-dY^2.$$

Так как x_0,y_0 – нечетные, а $d\equiv 1(\mathrm{mod}4)$, то $X=2X_0, Y=2Y_0$, где X_0,Y_0 – нечетные. Тогда, сокращая на 4, имеем

$$X_0^2-dY_0^2=4.$$

Следовательно, мы нашли нечетное решение уравнения $x^2 - dy^2 = 4$. Данное противоречие завершает доказательство. $\square$

Возьмем $y = 1, x = 2n + 1, n \in \mathbb{N} \cup \{0\}$ и подставим в уравнение $x^2 - dy^2 = -4$. Выразив d, получим

$$d = (2n + 1)^2 + 4 = 4n^2 + 4n + 5.$$

Или, подставив те же x и y в $x^2 - dy^2 = 4$, при $n \in \mathbb{N}$ имеем

$$d = (2n + 1)^2 - 4 = 4n^2 + 4n - 3.$$

При помощи данных формул можно получить некоторые бесквадратные значения d, при которых уравнение (***) разрешимо. Например, $d = 5, 13, 21, 29, 53, \ldots$. При этом, если d будет содержать квадрат какого-либо числа m, то m – нечетно. Значит, мы можем записать d в виде $d = d_1 m^2$, где d_1 – бесквадратное число. А тогда если (x_0, y_0) есть какое-то решение уравнения (***), то (x_0, my_0) – решение $x^2 - d_1 y^2 = \pm 4$.

Уравнение (***) не разрешимо, например, если $d = 37, 101$, поскольку в этих случаях наименьшие положительные решения уравнения $x^2 - dy^2 = 4$ равны $(146, 24)$ и $(402, 40)$, соответственно.

Итак, наше исследование в последний раз распадается на два случая.

Случай 2.1: t – нечетное и $U = \{\overline{1}\}$.

Следующее очевидное утверждение показывает, что случай $U = \{\overline{1}\}$ действительно реализуется.

Лемма 12. *Если уравнение $x^2 - y^2 d = \pm 4$ имеет только четные решения, то в $R/2R$ по модулю $2R$ поднимается только один обратимый элемент – $\overline{1}$.*

Для начала классифицируем инволюции при нечетной размерности матриц. Так как $U = \{\overline{1}\}$, то определение эквивалентности векторов $z = (z_1, \ldots, z_k)$, $h = (h_1, \ldots, h_k) \in (R/2R)^k$ запишем в виде

$$z \sim_{odd,U} h \Leftrightarrow \exists\ e_{ii}, c_{ij} \in R/2R \text{ такие, что}$$

$$h_i = z_i + e_i^2 + \sum_{j=1}^{i-1} c_{ij}^2 z_j.$$

Из того, что $R/2R$ – поле $\mathbb{F}_4$, следует, что для любого $c \in R/2R$, найдется $x \in R/2R$ такой, что $x^2 = c$.

Предложение 7. *Пусть $a = (a_1, \ldots, a_k), b = (b_1, \ldots, b_k) \in (R/2R)^k$. Тогда $a \sim_{odd,U} b$.*

Доказательство. Выберем произвольные элементы a_m, b_m где $1 \leqslant m \leqslant k$ и покажем, что будет выполняться равенство

$$a_m = b_m + e_m^2 + \sum_{j=1}^{m-1} c_{mj}^2 b_j,$$

для некоторых $e_m, c_{mj} \in R/2R$.

Какими бы ни были a_m и b_m мы всегда можем выбрать $e_m \in R/2R$ так, чтобы выполнялось равенство $a_m = b_m + e_m^2$. А это значит, что

$$a_m = b_m + e_m^2 + \sum_{j=1}^{m-1} c_{mj}^2 b_j,$$

где все $c_{mj} = \overline{0}$. $\square$

Итак, если $U = \{\overline{1}\}$, то в силу Предложения 7 и Теоремы 4 в $T_{2k+1}(\mathbb{Z}[\varphi])$ все инволюции попарно эквивалентны. Теперь посмотрим, что будет в случае четной размерности матриц. Запишем определение эквивилентных векторов $z = (z_1, \ldots, z_k)$, $h = (h_1, \ldots, h_k) \in (R/2R)^k$

$$z \sim_{even,U} h \Leftrightarrow \exists\ c_{ij} \in R/2R : h_i = z_i + \sum_{j=1}^{i-1} c_{ij}^2 z_j.$$

Как и прежде, нулевой вектор эквивалентен только себе.

Предложение 8. *Пусть* $a = (a_1, \ldots, a_s, \ldots, a_k) \in (R/2R)^k$ *– ненулевой. Тогда*

$a \sim_{even,U} z_s = (\overline{z_1}, \ldots, \overline{z_s}, \ldots, \overline{z_k}) \in (R/2R)^k$, *где* $\overline{z_s} \neq \overline{0}$, *а все остальные элементы равны* $\overline{0} \Leftrightarrow$

$$\Leftrightarrow \forall\ 1 \leqslant i < s\ a_i = \overline{0}\ u\ a_s = \overline{z_s}.$$

Доказательство. ($\Leftarrow$) Так как $\overline{z_i} = \overline{0}$ для любого индекса $1 \leqslant i < s$, следовательно, выполняется равенство

$$a_i = \overline{0} = \overline{0} + \sum_{j=1}^{i-1} c_{ij}^2 \cdot \overline{0} = \overline{z_i} + \sum_{j=1}^{i-1} c_{ij}^2 \overline{z_j},$$

для любых $c_{ij} \in R/2R$.

Выберем произвольный элемент a_m, где $s < m \leqslant k$ и покажем, что будет выполняться равенство

$$a_m = \overline{z_m} + \sum_{j=1}^{m-1} c_{mj}^2 \overline{z_j},$$

для некоторых $c_{mj} \in R/2R$. Действительно, выберем $c_{ms} \in R/2R$ так, чтобы выполнялось равенство $a_m = c_{ms}^2 \overline{z_s}$. Несложно проверить, такие c_{ms} существуют для любых значений a_m и $\overline{z_s}$. Теперь заметим, что

$$a_m = c_{ms}^2 \overline{z_s} = \overline{z_m} + \sum_{j=1}^{m-1} c_{mj}^2 \overline{z_j},$$

где $c_{mj} = \overline{0}$ при $j \neq s$. Для индекса s, имеем

$$a_s = \overline{z_s} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j},$$

для любых $c_{sj} \in R/2R$. ($\Rightarrow$) Пусть теперь $a \sim_{even,U} z_s$. Тогда для любого индекса $1 \leqslant l \leqslant k$ выполняется

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j}.$$

Причем, если $l < s$, то

$$a_l = \overline{z_l} + \sum_{j=1}^{l-1} c_{lj}^2 \overline{z_j} = \overline{0} + \sum_{j=1}^{l-1} c_{lj}^2 \cdot \overline{0} = \overline{0}.$$

Если же $l = s$, тогда

$$a_s = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \overline{z_j} = \overline{z_s} + \sum_{j=1}^{s-1} c_{sj}^2 \cdot \overline{0} = \overline{z_s}.$$

□

Только что доказанное утверждение влечет за собой, что $z_s \not\sim_{even,U} z_{s_1}$, если $z_s \neq z_{s_1}$ или $s \neq s_1$. Таким образом, из Предложения 8 следует, что любой ненулевой вектор в $(R/2R)^k$ эквивалентен одному из векторов вида z_s. Прямой подсчет показывает, что векторов типа z_s – $3k$ вариантов и один нулевой вектор, следовательно $|(R/2R)^k/\sim_{even,U}| = 3k+1$. И тогда, в силу Теоремы 4 и Следствия 1 [3], имеем $|\beta| = 3k+2$, где β – множество классов эквивалентности инволюций в $T_{2k}(\mathbb{Z}[\varphi])$.

Случай 2.2: t – нечетное и $U = \{\overline{1}, \overline{\varphi}, \overline{\varphi+1}\}$.

Если в $R/2R$ все обратимые элементы поднимаются по модулю $2R$, то из Следствия 4 [3] и Теоремы 4 [3] следует, что в $T_{2k+1}(\mathbb{Z}[\varphi])$ все инволюции попарно эквивалентны, а из Следствия 4 [3], Теоремы 3 [3] и Следствия 1 [3] следует, что в $T_{2k}(\mathbb{Z}[\varphi])$ ровно $(k+1)^2+1$ классов эквивалентности инволюций.

Таким образом, нами доказана **Теорема 3**.

5. Заключение

Для иллюстрации результатов, полученных в нашем исследовании, построим несколько примеров для алгебр $T_4(\mathbb{Z}[\sqrt{d}])$ и $T_5(\mathbb{Z}[\sqrt{d}])$.

Пример 1. *Пусть $d = -5$, т.е. $d \equiv 3(\mathrm{mod}4)$. Очевидно, что уравнение $x^2 + 5y^2 = 1$ не разрешимо при x – четном, y – нечетном. Следовательно, по Теореме 1 в алгебре $T_4(\mathbb{Z}[\sqrt{-5}])$ имеется ровно 14 классов эквивалентности инволюций, а в алгебре $T_5(\mathbb{Z}[\sqrt{-5}])$ — 3 класса эквивалентности инволюций.*

Пример 2. *Пусть $d = 26$, т.е. $d \equiv 2(\mathrm{mod}4)$. Уравнение $x^2 - 26y^2 = -1$, где x, y – нечетные, разрешимо (например при $x = 5, y = 1$). Следовательно, по Теореме 2 в алгебре $T_4(\mathbb{Z}[\sqrt{26}])$ имеется ровно 8 классов эквивалентности инволюций, а в алгебре $T_5(\mathbb{Z}[\sqrt{26}])$ — 3 класса эквивалентности инволюций.*

Пример 3. *Пусть $d = 37$, т.е. $d \equiv 1(\mathrm{mod}4)$. Так $d = 4 \cdot \boldsymbol{9} + 1$, то по Теореме 3 в алгебре $T_4(\mathbb{Z}[\sqrt{37}])$ имеется ровно 8 классов эквивалентности инволюций, а в алгебре $T_5(\mathbb{Z}[\sqrt{37}])$ все инволюции попарно эквивалентны.*

Помимо количества классов эквивалентности инволюций в конкретной алгебре верхнетреугольных матриц, безусловно, представляет интерес устройство инволюций в каждом таком классе. Следующий пример прольет свет на данный вопрос.

Пример 4. *Рассмотрим алгебру $T_2(\mathbb{Z}[\sqrt{-5}])$. По Теореме 1 в данной алгебре 5 классов эквивалентности инволюций. Очевидно, что представителями двух классов являются ортогональная и симплектическая инволюции. Чтобы найти представителей других трех классов обратимся к Предложению 3.*

Так как мы рассматриваем матрицы размера 2×2, то вектор z_s состоит из одной компоненты. При этом $a \sim_{even,U} z_s$ тогда и только тогда, когда $a = z_s$. Следовательно, $a = \overline{1}$ или $a = \overline{\varphi}$, или $a = \overline{\varphi+1}$. Берем по одному элементу из каждого смежного класса и получаем три неэквивалентных между собой инволюции. Для произвольной матрицы $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T_2(\mathbb{Z}[\sqrt{-5}])$ имеем:

1) $\gamma_{B_1}(A) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot A^* \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ *или* $\gamma_{B_1} : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & (a-c)+b \\ 0 & a \end{pmatrix}$;

2) $\gamma_{B_2}(A) = \begin{pmatrix} 1 & \sqrt{-5} \\ 0 & 1 \end{pmatrix} \cdot A^* \cdot \begin{pmatrix} 1 & -\sqrt{-5} \\ 0 & 1 \end{pmatrix}$ *или* $\gamma_{B_2} : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & \sqrt{-5}(a-c)+b \\ 0 & a \end{pmatrix}$;

3) $\gamma_{B_3}(A) = \begin{pmatrix} 1 & 1+\sqrt{-5} \\ 0 & 1 \end{pmatrix} \cdot A^* \cdot \begin{pmatrix} 1 & -1-\sqrt{-5} \\ 0 & 1 \end{pmatrix}$ *или*

$$\gamma_{B_3} : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & (1+\sqrt{-5})(a-c)+b \\ 0 & a \end{pmatrix}.$$

Если же рассмотреть алгебру $T_2(R)$, *где* $R = \mathbb{Z}[\sqrt{-1}]$ *— кольцо целых Гауссовых чисел, то Теореме 1 в данной алгебре 4 класса эквивалентности инволюций. Снова, представителями двух классов являются ортогональная и симплектическая инволюции. А согласно Предложению 5 представителями других двух классов могут выступать, например, следующие инволюции:*

1) $\gamma_{B_1}(A) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot A^* \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ *или* $\gamma_{B_1} : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & (a-c)+b \\ 0 & a \end{pmatrix}$;

2) $\gamma_{B_2}(A) = \begin{pmatrix} 1 & 1+\sqrt{-1} \\ 0 & 1 \end{pmatrix} \cdot A^* \cdot \begin{pmatrix} 1 & -1-\sqrt{-1} \\ 0 & 1 \end{pmatrix}$ *или*

$$\gamma_{B_2} : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & (1+\sqrt{-1})(a-c)+b \\ 0 & a \end{pmatrix}.$$

Заметим, что отображение $\gamma_{B_3} : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & \sqrt{-1}(a-c)+b \\ 0 & a \end{pmatrix}$, *где* $B_3 = \begin{pmatrix} 1 & \sqrt{-1} \\ 0 & 1 \end{pmatrix}$, *также будет инволюцией в* $T_2(\mathbb{Z}[\sqrt{-1}])$. *Но при этом, инволюции* γ_{B_1} *и* γ_{B_3} *эквивалентны между собой. Покажем это, воспользовавшись Леммой 1 [3].*

Далее вместо $\sqrt{-1}$ *будем писать* i. *По Лемме 1 [3] нам необходимо найти обратимую матрицу* $V \in T_2(\mathbb{Z}[i])$ *и обратимый* $\lambda \in \mathbb{Z}[i]$ *такие, чтобы выполнялось равенство*

$$VB_3V^* = \lambda B_1.$$

Положим $V = \begin{pmatrix} 1 & -i \\ 0 & -i \end{pmatrix}$ *и* $\lambda = -i$. *Обратными к ним будут соответственно матрица* $V^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & i \end{pmatrix}$ *и элемент* i. *Непосредственная проверка показывает, что следующее равенство верно*

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

В заключении коротко отметим, что задача, поставленная в начале статьи, достигнута: изучена проблема классификации инволюций в алгебре верхнетреугольных матриц над кольцом целых алгебраических чисел квадратичных полей; в ходе описания инволюций в вышеупомянутой алгебре были найдены эквивалентные формулировки условий в рамках теории уравнений Пелля [5].

Благодарности

Автор выражает искреннюю благодарность А. Н. Абызову, Д. Т. Тапкину и М. Е. Чанге за многочисленные обсуждения результатов и интерес к настоящей работе.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Крылов П. А., Норбосамбуев Ц. Д. Автоморфизмы алгебр формальных матриц // Сиб. мат. журнал, 2018, Т. 59, № 5, С. 1116–1127.
2. Крылов П. А., Туганбаев А. А. Группы автоморфизмов колец формальных матриц // Итоги науки и техн. Сер. Соврем. мат. и ее прил. Темат. обз., 2019, Т. 164, С. 96–124.
3. Кульгускин И. А., Тапкин Д. Т. Инволюции в алгебре верхнетреугольных матриц // Известие вузов. Математика, 2023, № 6, С. 11-30.
4. Ленг С. Алгебраические числа. — М.: Мир, 1966, 224 с.
5. Чанга М. Е. Элементарная теория уравнений Пелля. — Москва: МПГУ, 2019, 36 с.
6. Albert A. A. Structure of algebras. — Amer. Math. Soc. Colloquium Publ., 1961, Vol. 24, 210 p.
7. Brusamarello R., Fornaroli E. Z., Santulo Jr. E. A. Classication of involutions on incidence algebras // Comm. Alg., 2011, Vol. 39, P. 1941–1955.
8. Brusamarello R., Fornaroli E. Z., Santulo Jr. E. A. Anti-automorphisms and involutions on (finitary) incidence algebras // Linear Multilinear Algebra, 2012, Vol. 60, P. 181–188.
9. Brusamarello R., Lewis D. W. Automorphisms and involutions on incidence algebras // Linear and Multilinear Algebra, 2011, Vol. 59, No. 11, P. 1247–1267.
10. Fornaroli E. Z., Pezzott R. E. M. Anti-isomorphisms and involutions on the idealization of the incidence space over the finitary incidence algebra // Linear Algebra Appl, 2022, Vol. 637, P. 82–109.
11. Jacobson N. Finite-dimensional division algebras over fields. — Berlin, Springer-Verlag, 1996, 284 p.
12. Knus M. A., Merkurjev A., Rost M., Tignol J.-P. The Book of Involutions. — Amer. Math. Soc. Colloquium Publ., 1998, Vol. 44, 31 p.
13. Krylov P. A., Tuganbaev A. A. Automorphisms of Formal Matrix Rings // J. Math. Sci., 2021, Vol. 258, No. 2, P. 222–249.
14. Spiegel E. Involutions in incidence algebras // Linear Algebra App., 2005, Vol. 405, P. 155–162.
15. Vincenzo O. M., Koshlukov P., Scala R. Involutions for upper triangular matrix algebras // Advances in Applied Mathematics, 2006, Vol. 37, P. 541–568.

REFERENCES

1. Krylov, P. A. & Norbosambuyev, Ts. D. 2018, “Automorphisms of formal matrix algebras”, *Sib. mat. Journal*, vol. 59, no. 5, pp. 1116–1127.
2. Krylov, P. A. & Tuganbaev, A. A. 2019, “Groups of automorphisms of rings of formal matrices”, *Results of Science and Technology*, vol. 164, pp. 96–124.
3. Kulguskin, I. A. & Tapkin, D. T. 2023, “Involutions in the algebra of upper triangular matrices”, *News of universities. Mathematics*, no. 6, pp. 11–30.

4. Leng, S. 1966, "Algebraic numbers", *Moscow: Mir*, 1966, 224 p.

5. Changa, M. E. 2019, "Elementary theory of Pell equations", *Moscow: MPSU*, 36 p.

6. Albert, A. A. 1961, "Structure of algebras", *Amer. Math. Soc. Colloquium Publ.*, vol. 24, 210 p.

7. Brusamarello, R., Fornaroli, E. Z. & Santulo Jr. E. A. 2011, "Classication of involutions on incidence algebras", *Comm. Alg.*, vol. 39, pp. 1941–1955.

8. Brusamarello, R., Fornaroli, E. Z. & Santulo Jr. E. A. 2012, "Anti-automorphisms and involutions on (finitary) incidence algebras", *Linear Multilinear Algebra*, vol. 60, pp. 181–188.

9. Brusamarello, R. & Lewis, D. W. 2011, "Automorphisms and involutions on incidence algebras", *Linear and Multilinear Algebra*, vol. 59, no. 11, pp. 1247–1267.

10. Fornaroli, E. Z. & Pezzott, R. E. M. 2022, "Anti-isomorphisms and involutions on the idealization of the incidence space over the finitary incidence algebra", *Linear Algebra Appl*, vol. 637, pp. 82–109.

11. Jacobson, N. 1996, "Finite-dimensional division algebras over fields", *Berlin: Springer-Verlag*, 284 p.

12. Knus, M. A., Merkurjev, A., Rost, M. & Tignol, J.-P. 1998, "The Book of Involutions", *Amer. Math. Soc. Colloquium Publ.*, vol. 44, 31 p.

13. Krylov, P. A. & Tuganbaev, A. A. 2021, "Automorphisms of Formal Matrix Rings", *J. Math. Sci.*, vol. 258, no. 2, pp. 222–249.

14. Spiegel, E. 2005, "Involutions in incidence algebras", *Linear Algebra App.*, vol. 405, pp. 155–162.

15. Vincenzo, O. M., Koshlukov, P. & Scala, R. 2006, "Involutions for upper triangular matrix algebras", *Advances in Applied Mathematics*, vol. 37, pp. 541–568.

Получено: 06.10.2023
Принято в печать: 21.12.2023