ВЕСТНИК ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2024 Математика и механика № 91
Tomsk State University Journal of Mathematics and Mechanics

Научная статья
УДК 512.552 MSC: 08A35, 15B99, 16S50
doi: 10.17223/19988621/91/3

Нильпотентные, ниль-хорошие и ниль-чистые формальные матрицы над кольцами вычетов

Анастасия Максимовна Елфимова[1], Цырендоржи Дашацыренович Норбосамбуев[2], Максим Вадимович Подкорытов[3]

[1, 2, 3] *Томский государственный университет, Томск, Россия*
[1] *elfimova.nastya@bk.ru*
[2] *nstsddts@yandex.ru*
[3] *maximthegreate@yandex.ru*

Аннотация. Продолжена работа над аддитивными задачами в кольцах формальных матриц над кольцами вычетов. Найдены необходимые и достаточные условия нильпотентности формальной матрицы над кольцами вычетов, показано, что кольцо таких матриц будет (p – 1)-ниль-чистым и ниль-хорошим чистым. Также, отвечая на вопрос, поставленный в статье второго соавтора, мы доказали, что кольцо формальных матриц над кольцами вычетов никогда не ниль-хорошее, а следовательно, и не изящное.

Ключевые слова: кольцо формальных матриц, нильпотентная формальная матрица, ниль-хорошее кольцо, изящное кольцо, ниль-чистое кольцо, ниль-хорошее чистое кольцо, кольцо контекста Мориты

Благодарности: Работа выполнена в рамках проекта «Кольца, близкие к хорошим» во время Большой математической мастерской в Томском государственном университете при финансовой поддержке Министерства науки и высшего образования РФ (соглашение № 075-02-2024-1437).

Для цитирования: Елфимова А.М., Норбосамбуев Ц.Д., Подкорытов М.В. Нильпотентные, ниль-хорошие и ниль-чистые формальные матрицы над кольцами вычетов // Вестник Томского государственного университета. Математика и механика. 2024. № 91. С. 31–40. doi: 10.17223/19988621/91/3

Original article

Nilpotent, nil-good, and nil-clean formal matrices over residue class rings

Anastasia M. Elfimova[1], Tsyrendorzhi D. Norbosambuev[2], Maxim V. Podkorytov[3]

[1, 2, 3] *Tomsk State University, Tomsk, Russian Federation*
[1] *elfimova.nastya@bk.ru*

[2] nstsddts@yandex.ru
[3] maximthegreate@yandex.ru

Abstract. Let us recall some classes of rings. A ring R is said to be k-nil-clean if each element can be written as a sum of a nilpotent and k idempotents. A ring R is said to be fine if each non-zero element can be written as a sum of a unit and a nilpotent. A ring R is called nil-good if every element is a nilpotent or a sum of a nilpotent and a unit. And, finally, ring R is called nil-good clean if every element is a sum of a nilpotent, an idempotent, and a unit.

In this paper, we continue our work on additive problems in formal matrix rings over residue class rings. We have found necessary and sufficient conditions for the nilpotency of a formal matrix over residue class rings. After that we have shown that a ring of such matrices is $(p-1)$-nil-clean and nil-good clean. Also, answering the question posed in the previous article of the second co-author, we prove that a ring of formal matrices over residue rings is never nil-good, and, therefore, not fine.

Let p be a prime, m and n be natural numbers, $m > n > 0$. Consider the ring of formal matrices over residue class rings $K = \begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \end{pmatrix} = \left\{ \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \middle| a,b,c,d \in \mathbf{Z} \right\}$

where for all $A, A' \in K$

$$A \cdot A' = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \cdot \begin{pmatrix} a'+p^m\mathbf{Z} & b'+p^n\mathbf{Z} \\ c'+p^n\mathbf{Z} & d'+p^n\mathbf{Z} \end{pmatrix} =$$

$$= \begin{pmatrix} aa'+p^{m-n}bc'+p^m\mathbf{Z} & ab'+bd'+p^n\mathbf{Z} \\ ca'+dc'+p^n\mathbf{Z} & p^{m-n}cb'+dd'+p^n\mathbf{Z} \end{pmatrix}.$$

One can see that the ring K is isomorphic to the endomorphism ring of the abelian group $((\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z}), +)$.

Theorem 2.1. Let $A = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \in K$. Matrix A is nilpotent if and only if a and d are multiples of p.

Corollary 2.3. Ring K is not nil-good.

Corollary 2.4. Ring K is not fine.

Theorem 3.5. Ring K is $(p-1)$-nil-clean.

Corollary 3.6. $\begin{pmatrix} \mathbf{Z}/2^m\mathbf{Z} & \mathbf{Z}/2^n\mathbf{Z} \\ \mathbf{Z}/2^n\mathbf{Z} & \mathbf{Z}/2^n\mathbf{Z} \end{pmatrix}$ is a nil-clean ring.

Question 3.7. Will K be nil-clean for $p > 2$?

Problem 3.8. Find necessary and sufficient conditions for the idempotency of a matrix from K.

Proposition 3.9. Ring K is nil-good clean.

Keywords: formal matrix ring, nilpotent formal matrix, nil-good ring, fine ring, nil-clean ring, nil-good clean ring, Morita context ring

Acknowledgments: This work was supported by the Ministry of Science and Higher Education of Russia (agreement No. 075-02-2024-1437).

For citation: Elfimova, A.M., Norbosambuev, T.D., Podkorytov, M.V. (2024) Nilpotent, nil-good, and nil-clean formal matrices over residue class rings. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics*. 91. pp. 31–40. doi: 10.17223/19988621/91/3

Введение

Все рассматриваемые кольца – ассоциативные с единицей, $E(G)$ – кольцо эндоморфизмов абелевой группы G, $U(R)$ – группа обратимых элементов кольца R, $M(n, R)$ – кольцо всех матриц порядка n над кольцом R, $\mathbf{Z}$ – кольцо (и группа) целых чисел, $\mathbf{Z}/p^n\mathbf{Z}$ – кольцо (и группа) вычетов по модулю p^n, ■ – конец доказательства или его отсутствие.

1. Формальные матрицы над кольцами вычетов

Пусть R и S – кольца, ${}_RM_S$ и ${}_SN_R$ – бимодули. Напомним, что *кольцом формальных матриц* (второго порядка) мы называем множество

$$K=\left\{\left.\begin{pmatrix} r & m \\ n & s \end{pmatrix}\right| r\in R, m\in {}_RM_S, n\in {}_SN_R, s\in S\right\}$$

с операциями поэлементного сложения и умножения вида:

$$\begin{pmatrix} r & m \\ n & s \end{pmatrix}\cdot\begin{pmatrix} r' & m' \\ n' & s' \end{pmatrix}=\begin{pmatrix} rr'+\varphi(m\otimes n') & rm'+ms' \\ nr'+sn' & \psi(n\otimes m')+ss' \end{pmatrix},$$

задаваемого с помощью бимодульных гомоморфизмов $\varphi: M\otimes_S N\to R$ и $\psi: N\otimes_R M\to S$. Также здесь нужно потребовать выполнения равенств $\varphi(m\otimes n)\cdot m'=m\cdot\psi(n\otimes m')$ и $\psi(n\otimes m)\cdot n'=n\cdot\varphi(m\otimes n')$, $m,m'\in M$, $n,n'\in N$, для ассоциативности умножения. Часто такое кольцо обозначают $K=\begin{pmatrix} R & M \\ N & S \end{pmatrix}$. Кольца формальных матриц, также называемые *кольцами контекста Мориты*, впервые появляются в работе японского математики Киити Мориты [1]. Для более подробного ознакомления с историей изучения контекста Мориты рекомендуем обзорную статью [2].

Пусть p – простое число, m и n – натуральные, $m\ge n>0$. Рассмотрим кольцо формальных матриц, в котором $R=\mathbf{Z}/p^m\mathbf{Z}$, $S=\mathbf{Z}/p^n\mathbf{Z}$, $M=\mathbf{Z}/p^n\mathbf{Z}$, $N=\mathbf{Z}/p^n\mathbf{Z}$, $\varphi((b+p^n\mathbf{Z})\otimes(c'+p^n\mathbf{Z}))=p^{m-n}bc'+p^m\mathbf{Z}$ и $\psi((c+p^n\mathbf{Z})\otimes(b'+p^n\mathbf{Z}))=p^{m-n}cb'+p^n\mathbf{Z}$ для любых b, c, b', $c'\in\mathbf{Z}$. Тогда получаем кольцо

$$K=\begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \end{pmatrix}=\left\{\left.\begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix}\right| a,b,c,d\in\mathbf{Z}\right\},$$

где для любых A, $A'\in K$

$$A\cdot A'=\begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix}\cdot\begin{pmatrix} a'+p^m\mathbf{Z} & b'+p^n\mathbf{Z} \\ c'+p^n\mathbf{Z} & d'+p^n\mathbf{Z} \end{pmatrix}=$$

$$=\begin{pmatrix} aa'+p^{m-n}bc'+p^m\mathbf{Z} & ab'+bd'+p^n\mathbf{Z} \\ ca'+dc'+p^n\mathbf{Z} & p^{m-n}cb'+dd'+p^n\mathbf{Z} \end{pmatrix}.$$

При $m=n$, конечно, $K=M(2, \mathbf{Z}/p^n\mathbf{Z})$. Этот случай нам не так интересен. Далее считаем, что $m>n$, если не отмечено иное.

Рассмотрим группу $((\mathbf{Z}/p^m\mathbf{Z})\oplus(\mathbf{Z}/p^n\mathbf{Z}), +)$. В работе [3] было показано, что кольцо эндоморфизмов группы $((\mathbf{Z}/p^m\mathbf{Z})\oplus(\mathbf{Z}/p^n\mathbf{Z}), +)$ изоморфно кольцу формальных мат-

риц $K = \begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \end{pmatrix}$. А именно, эндоморфизму θ группы $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z})$ соответствует единственная матрица $\begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \in K$ такая, что для любых $z_1, z_2 \in \mathbf{Z}$ имеет место равенство $\theta\begin{pmatrix} z_1+p^m\mathbf{Z} \\ z_2+p^n\mathbf{Z} \end{pmatrix} = \begin{pmatrix} az_1+p^{m-n}bz_2+p^m\mathbf{Z} \\ cz_1+dz_2+p^n\mathbf{Z} \end{pmatrix}$. Здесь элементы группы $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z})$ для наглядности записаны в столбец. Ясно также, что тождественному эндоморфизму соответствует матрица $E = \begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 1+p^n\mathbf{Z} \end{pmatrix}$.

Вместе с тем всякая конечная p-группа ранга 2 изоморфна группе вида $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z})$, где $m \geq n > 0$. Таким образом, кольца формальных матриц K второго порядка суть в точности кольца эндоморфизмов конечных p-групп второго ранга. Далее в статье можем не делать различий между кольцом формальных матриц K и кольцом эндоморфизмов $E((\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z}))$.

Кольца формальных матриц над кольцами вычетов подробно рассматриваются в статьях [3] и [4], также им уделяют внимание в работах [5–7]. Имеет место следующий критерий обратимости в кольце формальных матриц K.

Теорема 1.1 [3, 7]. Матрица $A = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \in K$ обратима тогда и только тогда, когда числа a и d не делятся на p. ■

Кольца формальных матриц над кольцами вычетов могут представлять интерес как основа для построения некоммутативного протокола шифрования данных. Этот раздел криптографии – некоммутативная алгебраическая криптография – в последнее время привлекает большой интерес специалистов по шифрованию данных. Кольцо K, очевидно, не является коммутативным, однако оно рассматривается над несколькими коммутативными кольцами $\mathbf{Z}/p^n\mathbf{Z}$, весьма просто устроенными. Также кольца K при $m > n$ не изоморфны кольцам обычных матриц $M(2, R)$. На данный момент предпринималось несколько попыток сконструировать протоколы шифрования, использующие кольца формальных матриц (см.: [8–11]).

2. Нильпотентные и ниль-хорошие формальные матрицы над кольцами вычетов

Пусть k – натуральное, $k > 1$. Напомним, что элемент кольца мы называем *k-хорошим*, если его можно записать в виде суммы k обратимых элементов этого кольца. Кольцо называем k-хорошим, если все его элементы таковы. Если все элементы кольца k-хороши, но для разных натуральных k, т.е. невозможно подобрать одно такое k, что все элементы являются k-хорошими, то называем кольцо в таком случае ω-хорошим. А если в кольце есть элементы, непредставимые в виде конечной суммы обратимых, то говорим, что кольцо не является хорошим.

Изучение колец, аддитивно порождаемых своими обратимыми элементами, началось с середины прошлого века. Эта тема вызывает интерес многих специалистов по алгебре. Выделим связанные с ней вопросы:

1. *Изящность* элемента кольца – возможность записать его как сумму нильпотентного и обратимого элементов. Кольцо называем изящным, если все его элементы, кроме нулевого, изящны. Если в кольце есть ненулевые элементы, непредставимые в виде суммы нильпотента и обратимого, то говорим, что кольцо не является изящным.

2 *Ниль-хорошесть* элемента кольца – возможность записать его как сумму нильпотента и элемента, который либо обратим, либо равен нулю кольца. Кольцо называем ниль-хорошим, если все его элементы таковы. Если в кольце есть хотя бы один не ниль-хороший элемент, то и все кольцо называем не ниль-хорошим.

3. *k-ниль-хорошесть* элемента кольца – возможность записать его в виде суммы одного нильпотентного и k обратимых элементов. Кольцо называем k-ниль-хорошим, если все его элементы таковы. Здесь, как и в случае с k-хорошестью, если все элементы кольца k-ниль-хороши, но для разных k, то называем кольцо в таком случае ω-ниль-хорошим.

Очевидно, что из изящности следует ниль-хорошесть. Из k-хорошести вытекает k-ниль-хорошесть. Подробнее об этих свойствах можно прочитать в работах [4] и [12] и в литературе, упоминаемой в них.

При $p > 2$ кольцо K является 2-хорошим [4], а значит и 2-ниль-хорошим. Вместе с тем при $p = 2$ кольцо K не является хорошим, т.е. в K найдутся матрицы, непредставимые в виде сумм конечного числа обратимых матриц. Также в [4] был задан вопрос: будет ли $E((\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z}))$ изящным или хотя бы ниль-хорошим кольцом? Что можно сказать о ниль-хорошести и изящности кольца $E((\mathbf{Z}/2^m\mathbf{Z}) \oplus (\mathbf{Z}/2^n\mathbf{Z}))$, $m > n$?

Для ответа на эти вопросы нужно знать необходимые и достаточные условия нильпотентности формальных матриц в K. Нам удалось их получить.

Теорема 2.1. Пусть $A = \begin{pmatrix} a + p^m\mathbf{Z} & b + p^n\mathbf{Z} \\ c + p^n\mathbf{Z} & d + p^n\mathbf{Z} \end{pmatrix} \in K$. Матрица A нильпотентна тогда и только тогда, когда числа a и d кратны p.

Доказательство. Пусть A – нильпотентная матрица, т.е. $A^k = 0$ для какого-то натурального k. Легко показать по индукции, что при любом натуральном i матрица A^i имеет вид:

$$A^i = \begin{pmatrix} a^i + p^{m-n}(\ldots) + p^m\mathbf{Z} & (\ldots) + p^n\mathbf{Z} \\ (\ldots) + p^n\mathbf{Z} & d^i + p^{m-n}(\ldots) + p^n\mathbf{Z} \end{pmatrix}.$$

Таким образом, для того чтобы элементы на главной диагонали матрицы A^k получились нулевыми (в смысле колец $\mathbf{Z}/p^m\mathbf{Z}$ и $\mathbf{Z}/p^n\mathbf{Z}$), числа a и d должны быть кратны p.

Обратно, пусть a и d кратны p. Тогда существуют такие числа a' и d', что $a = pa'$ и $d = pd'$. Вычислим A^2:

$$A^2 = \begin{pmatrix} a^2 + p^{m-n}bc + p^m\mathbf{Z} & ab + bd + p^n\mathbf{Z} \\ ca + dc + p^n\mathbf{Z} & p^{m-n}cb + d^2 + p^n\mathbf{Z} \end{pmatrix}.$$

Далее можем расписать

$$a^2 + p^{m-n}bc = pa'a + p \cdot p^{m-n-1}bc = p(a'a + p^{m-n-1}bc),$$
$$ab + bd = pa'b + bpd' = p(a'b + bd'),$$
$$ca + dc = cpa' + pd'c = p(ca' + d'c),$$
$$p^{m-n}cb + d^2 = p \cdot p^{m-n-1}cb + pd'd = p(p^{m-n-1}cb + d'd).$$

Итак,

$$A^2 = \begin{pmatrix} p(a'a + p^{m-n-1}bc) + p^m\mathbf{Z} & p(a'b + bd') + p^n\mathbf{Z} \\ p(ca' + d'c) + p^n\mathbf{Z} & p(p^{m-n-1}bc + d'd) + p^n\mathbf{Z} \end{pmatrix}.$$

Снова пользуясь индукцией, легко показать, что при любом натуральном i

$$A^{2i} = \begin{pmatrix} p^i(\ldots) + p^m\mathbf{Z} & p^i(\ldots) + p^n\mathbf{Z} \\ p^i(\ldots) + p^n\mathbf{Z} & p^i(\ldots) + p^n\mathbf{Z} \end{pmatrix}.$$

Тогда можем заключить, что по крайней мере

$$A^{2m} = \begin{pmatrix} p^m(\ldots) + p^m\mathbf{Z} & p^m(\ldots) + p^n\mathbf{Z} \\ p^m(\ldots) + p^n\mathbf{Z} & p^m(\ldots) + p^n\mathbf{Z} \end{pmatrix} = \begin{pmatrix} 0 + p^m\mathbf{Z} & 0 + p^n\mathbf{Z} \\ 0 + p^n\mathbf{Z} & 0 + p^n\mathbf{Z} \end{pmatrix}. \blacksquare$$

Следствие 2.2. Нильпотентные матрицы кольца K образуют идеал. ■

Далее, зная условия нильпотентности матриц в K, можем вывести следующий факт.

Следствие 2.3. K – не ниль-хорошее кольцо.

Доказательство. Пусть $A \in K$ – не нильпотентная и необратимая матрица. Такие матрицы существуют, это легко вывести из теорем 1.1 и 2.1. Допустим, что A – ниль-хорошая, тогда $A = N + 0$ или $A = N + U$, где N – нильпотентная, U – обратимая матрицы. В первом случае получаем, что A – нильпотентная, что противоречит нашему предположению. Пусть $A = N + U$, тогда по теореме 2.1 и теореме 1.1 матрицы N и U имеют вид:

$$N = \begin{pmatrix} pa + p^m\mathbf{Z} & b + p^n\mathbf{Z} \\ c + p^n\mathbf{Z} & pd + p^n\mathbf{Z} \end{pmatrix},\ U = \begin{pmatrix} a' + p^m\mathbf{Z} & b' + p^n\mathbf{Z} \\ c' + p^n\mathbf{Z} & d' + p^n\mathbf{Z} \end{pmatrix},$$

где a, a', b, b', c, c', d, $d' \in \mathbf{Z}$, причем a' и d' не делятся на p. Тогда, как несложно видеть,

$$A = \begin{pmatrix} a' + pa + p^m\mathbf{Z} & b + b' + p^n\mathbf{Z} \\ c + c' + p^n\mathbf{Z} & d' + pd + p^n\mathbf{Z} \end{pmatrix} \in U(K),$$

что противоречит нашему предположению, что A – необратимая матрица. Значит, A не может быть ниль-хорошей. Следовательно, K – не ниль-хорошее кольцо. ■

Как мы отмечали выше, изящное кольцо всегда будет ниль-хорошим. Следовательно, кольцо, не являющееся ниль-хорошим, не может быть изящным.

Следствие 2.4. Кольцо K не изящно. ■

Таким образом, мы ответили на оба вопроса, поставленных ранее в [4]: кольцо формальных матриц K не будет ни изящным, ни ниль-хорошим ни при каком простом p.

Заметим, однако, что при $m = n$ и $p = 2$ кольцо $K = M(2, \mathbf{Z}/2^n\mathbf{Z})$ – 2-ниль-хорошее, ниль-хорошее, но не изящное [4. Предложение 3.11].

3. Чистые, ниль-чистые и ниль-хорошие чистые формальные матрицы над кольцами вычетов

Напомним, что элемент кольца называется *чистым*, если его можно разложить в сумму идемпотентного и обратимого элементов кольца. Кольцо называем чистым, если все его элементы чистые. Со свойством чистоты также связаны понятия:

1. *Ниль-чистота* – элемент кольца называем ниль-чистым, если его можно разложить в сумму идемпотентного и нильпотентного элементов кольца. Кольцо называем ниль-чистым, если все его элементы ниль-чисты.

2. *k-ниль-чистота* – элемент кольца называем *k*-ниль-чистым, если его можно разложить в сумму одного нильпотентного и *k* идемпотентных элементов кольца, где *k* – натуральное число. Кольцо называем *k*-ниль-чистым, если все его элементы *k*-ниль-чисты.

3. *Ниль-хорошая чистота* – элемент кольца называем ниль-хорошим чистым, если его можно разложить в сумму идемпотентного, нильпотентного и обратимого элементов кольца. Кольцо называем ниль-хорошим чистым, если все его элементы ниль-хорошие чистые.

Для более подробного ознакомления с этими свойствами см. литературу, упоминаемую, например, в [4] и [12].

Теорема 3.1 [5]. Если R и S – чистые кольца, то кольцо формальных матриц $\begin{pmatrix} R & M \\ N & S \end{pmatrix}$ – тоже чистое. ■

Поскольку при любых простых p и $n \in \mathbf{N}$ кольцо $\mathbf{Z}/p^n\mathbf{Z}$ является чистым, то получаем

Следствие 3.2. Кольцо K – чистое. ■

Следующее утверждение можно проверить непосредственно.

Лемма 3.3. Для любого простого p и для любых натуральных m и n, $m \geq n$, следующие (формальные) матрицы являются нетривиальными идемпотентами в K:

$$\begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}, \begin{pmatrix} 0+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 1+p^n\mathbf{Z} \end{pmatrix}, \begin{pmatrix} 1+p^m\mathbf{Z} & 1+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix},$$

$$\begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 1+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}, \begin{pmatrix} 0+p^m\mathbf{Z} & 1+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 1+p^n\mathbf{Z} \end{pmatrix}, \begin{pmatrix} 0+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 1+p^n\mathbf{Z} & 1+p^n\mathbf{Z} \end{pmatrix}. \blacksquare$$

Лемма 3.4. Если элемент кольца ниль-чист, то он будет и *k*-ниль-чист для любого $k \geq 1$.

Действительно, пусть $a = n + e$, где n – нильпотент, e – идемпотент. Тогда $a = n + e + 0 + \ldots + 0$ – *k*-ниль-чистое разложение элемента a с $k - 1$ нулевыми слагаемыми. ■

Теорема 3.5. Кольцо K является $(p - 1)$-ниль-чистым.

Доказательство. Пусть $A = \begin{pmatrix} x+pa+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & y+pd+p^n\mathbf{Z} \end{pmatrix} \in K$, где $a, b, c, d, x,$ $y \in \mathbf{Z}$, причем $0 \leq x < p$ и $0 \leq y < p$. Считаем, что $x \geq y$ (случай $x \leq y$ рассматривается аналогично). Тогда можем записать

$$A = \begin{pmatrix} pa+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & pd+p^n\mathbf{Z} \end{pmatrix} + \sum_{y \text{ раз}} \begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 1+p^n\mathbf{Z} \end{pmatrix} + \\ + \sum_{x-y \text{ раз}} \begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}. \quad (1)$$

Получили сумму одной нильпотентной и x идемпотентных матриц. Понятно, что если $x = y$, то слагаемых вида $\begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}$ в разложении (1) просто не будет. Далее, поскольку $x < p$, $y < p$, то слагаемых $\begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 1+p^n\mathbf{Z} \end{pmatrix}$ и $\begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}$ в разложении (1) матрицы A не может быть больше $p - 1$. А если таких слагаемых меньше $p - 1$, то всегда можно добавить нужное количество нулевых матриц (см. лемму 3.4). ■

Следствие 3.6. Кольцо $K = \begin{pmatrix} \mathbf{Z}/2^m\,\mathbf{Z} & \mathbf{Z}/2^n\,\mathbf{Z} \\ \mathbf{Z}/2^n\,\mathbf{Z} & \mathbf{Z}/2^n\,\mathbf{Z} \end{pmatrix}$ – ниль-чистое.

Вопрос 3.7. Может ли K быть ниль-чистым кольцом при $p > 2$?

Для ответа на этот вопрос нужно знать, когда формальная матрица $A \in K$ является идемпотентной.

Проблема 3.8. Найти необходимые и достаточные условия идемпотентности матриц из K.

В завершение установим ниль-хорошую чистоту кольца K.

Предложение 3.9. Кольцо K является ниль-хорошим чистым.

Доказательство. Если $A \in K$ – обратимая матрица, то можем записать $A = 0 + 0 + A$; таким образом, A – ниль-хорошая чистая.

Если матрица $A \in K$ нильпотентна, то можем записать $A = A + E + (-E)$ – сумма нильпотентной, идемпотентной и обратимой матриц.

Пусть $A \in K$ – не нильпотентная и необратимая матрица. Тогда $A = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix}$, где либо a делится на p и d не делится на p, либо d делится на p и a не делится на p. Для определенности пусть a делится на p и d не делится. Полагая

$$X = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}, \quad Y = \begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & 0+p^n\mathbf{Z} \end{pmatrix}, \quad Z = \begin{pmatrix} -1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} \\ 0+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix},$$

получаем, что $A = X + Y + Z$, где матрица X нильпотентна в силу теоремы 2.1, матрица Y идемпотентна по лемме 3.3, и матрица Z обратима в силу теоремы 1.1. ■

Список источников

1. *Morita K.* Duality for modules and its applications to the theory of rings with minimum condition // Sci. Rep. Tokyo Kyoiku Daigaku. Sect. A. 1958. V. 6. P. 83–142.
2. *Loustaunau P.*, *Shapiro J.* Morita contexts // Non-Commutative Ring Theory. Springer, 1990. P. 80–92. (Lecture Notes in Mathematics; v. 1448). doi: 10.1007/BFb0091253
3. *Степанова А.Ю.*, *Тимошенко Е.А.* Матричное представление эндоморфизмов примарных групп малых рангов // Вестник Томского государственного университета. Математика и механика. 2021. № 74. С. 30–42. doi: 10.17223/19988621/74/4
4. *Норбосамбуев Ц.Д.* Хорошие кольца формальных матриц над кольцами вычетов // Вестник Томского государственного университета. Математика и механика. 2023. № 85. С. 32–42. doi: 10.17223/19988621/85/3

5. *Крылов П.А.*, *Туганбаев А.А.* Кольца формальных матриц и модули над ними. М. : МЦНМО, 2017.
6. *Крылов П.А.*, *Туганбаев А.А.* Формальные матрицы и их определители // Фундаментальная и прикладная математика. 2014. № 1 (19). С. 65–119.
7. *Крылов П.А.* Определители обобщенных матриц порядка 2 // Фундаментальная и прикладная математика. 2015. № 5 (20). С. 95–112.
8. *Climent J.-J., Navarro P.R., Tortosa L.* Key exchange protocols over noncommutative rings. The case of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ // International Journal of Computer Mathematics. 2012. V. 89. P. 1753–1763. doi: 10.1080/00207160.2012.696105
9. *Climent J.-J., López-Ramos J.A.* Public key protocols over the ring $E_p^{(m)}$ // Advances in Mathematics of Communications. 2016. V. 10. P. 861–870.
10. *Long D.T., Thu D.T., Thuc D.N.* A Bergman ring based cryptosystem analogue of RSA // International Conference on IT Convergence and Security, ICITCS 2013. doi: 10.1109/ICITCS.2013.6717769
11. *Farida N.J., Irawati*. On the arithmetic of endomorphism ring $\mathrm{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ and its RSA variants // South East Asian Journal of Mathematics and Mathematical Sciences. 2023. V. 19 (2). P. 53–64. doi: 10.56827/SEAJMMS.2023.1902.4
12. *Норбосамбуев Ц.Д., Тимошенко Е.А.* О *k*-ниль-хороших кольцах формальных матриц // Вестник Томского государственного университета. Математика и механика. 2022. № 77. С. 17–26. doi: 10.17223/19988621/77/2

References

1. Morita K. (1958) Duality for modules and its applications to the theory of rings with minimum condition. *Science Reports of the Tokyo Kyoiku Daigaku*, *Section A.* 6. pp. 83–142.
2. Loustaunau P., Shapiro J. (1990) Morita contexts. *Non-Commutative Ring Theory* (Lecture Notes in Mathematics, Vol. 1448). Springer. pp. 80–92. DOI: 10.1007/BFb0091253.
3. Stepanova A.Yu., Timoshenko E.A. (2021) Matrichnoye predstavleniye endomorfizmov primarnykh grupp malykh rangov [Matrix representation of endomorphisms of primary groups of small ranks]. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics*. 74. pp. 30–42. DOI: 10.17223/19988621/74/4.
4. Norbosambuev T.D. (2023) Khoroshiye kol'tsa formal''nykh matrits nad kol'tsami vychetov [Good formal matrix rings over residue class rings]. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics*. 85. pp. 32–42. DOI: 10.17223/19988621/85/3.
5. Krylov P., Tuganbaev A. (2017) *Formal Matrices*. (Algebra and Applications, Vol. 23). Springer. DOI: 10.1007/978-3-319-53907-2.
6. Krylov P.A., Tuganbaev A.A. (2015) Formal matrices and their determinants. *Journal of Mathematical Sciences* (*New York*). 211(3). pp. 341–380. DOI: 10.1007/s10958-015-2610-3.
7. Krylov P.A. (2018) Determinants of generalized matrices of order 2. *Journal of Mathematical Sciences* (*New York*). 230(3). pp. 414–427. DOI: 10.1007/s10958-018-3748-6.
8. Climent J.-J., Navarro P.R., Tortosa L. (2012) Key exchange protocols over noncommutative rings. The case of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *International Journal of Computer Mathematics*. 89. pp. 1753–1763. DOI: 10.1080/00207160.2012.696105.
9. Climent J.-J., López-Ramos J.A. (2016) Public key protocols over the ring $E_p^{(m)}$. *Advances in Mathematics of Communications*. 10. pp. 861–870.
10. Long D.T., Thu D.T., Thuc D.N. (2013) A Bergman ring based cryptosystem analogue of RSA. *International Conference on IT Convergence and Security, ICITCS*. DOI: 10.1109/ICITCS.2013.6717769.

11. Farida N.J., Irawati (2023) On the arithmetic of endomorphism ring $\mathrm{End}(\mathbb{Z}_{p^2} \times \mathbb{Z}_p)$ and its RSA variants. *South East Asian Journal of Mathematics and Mathematical Sciences*. 19(2). pp. 53–64. DOI: 10.56827/SEAJMMS.2023.1902.4.
12. Norbosambuev T.D., Timoshenko E.A. (2022) O *k*-nil'-khoroshikh kol'tsakh formal'nykh matrits [On k-nil-good formal matrix rings]. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics.* 77. pp. 17–26. DOI: 10.17223/19988621/77/2.

***Сведения об авторах*:**
Елфимова Анастасия Максимовна – аспирант механико-математического факультета Томского государственного университета (Томск, Россия). E-mail: elfimova.nastya@bk.ru
Норбосамбуев Цырендоржи Дашацыренович – кандидат физико-математических наук, доцент кафедры алгебры механико-математического факультета Томского государственного университета, старший научный сотрудник Регионального научно-образовательного математического центра Томского государственного университета (Томск, Россия). E-mail: nstsddts@yandex.ru
Подкорытов Максим Вадимович – студент механико-математического факультета Томского государственного университета (Томск, Россия). E-mail: maximthegreate@yandex.ru

***Information about the authors*:**
Elfimova Anastasia M. (Tomsk State University, Tomsk, Russian Federation). E-mail: elfimova.nastya@bk.ru
Norbosambuev Tsyrendorzhi D. (Candidate of Physics and Mathematics, Tomsk State University, Tomsk, Russian Federation). E-mail: nstsddts@yandex.ru
Podkorytov Maxim V. (Tomsk State University, Tomsk, Russian Federation). E-mail: maximthegreate@yandex.ru

Статья поступила в редакцию 28.02.2024; принята к публикации 03.10.2024

The article was submitted 28.02.2024; accepted for publication 03.10.2024