ВЕСТНИК ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2025 Математика и механика № 94
Tomsk State University Journal of Mathematics and Mechanics

Научная статья
УДК 512.541+512.552 MSC: 16S50
doi: 10.17223/19988621/94/5

Кольца обобщенных матриц, представляющих эндоморфизмы конечной примарной группы

Александра Юрьевна Степанова[1], Егор Александрович Тимошенко[2]

[1, 2] Томский государственный университет, Томск, Россия
[1] stepanova.alexa@mail.ru
[2] tea471@mail.tsu.ru

Аннотация. Для кольца эндоморфизмов конечной примарной группы построено изоморфное ему кольцо обобщенных матриц. Установлен критерий обратимости таких обобщенных матриц, описан алгоритм нахождения обратной матрицы в указанном кольце.
Ключевые слова: примарная группа, кольцо эндоморфизмов, кольцо обобщенных матриц, обратная матрица

Благодарности: Работа выполнена при поддержке Министерства науки и высшего образования РФ (соглашение № 075-02-2025-1728/2).

Для цитирования: Степанова А.Ю., Тимошенко Е.А. Кольца обобщенных матриц, представляющих эндоморфизмы конечной примарной группы // Вестник Томского государственного университета. Математика и механика. 2025. № 94. С. 57–66. doi: 10.17223/19988621/94/5

Original article

Rings of generalized matrices representing endomorphisms of a finite primary group

Aleksandra Yu. Stepanova[1], Egor A. Timoshenko[2]

[1, 2] Tomsk State University, Tomsk, Russian Federation
[1] stepanova.alexa@mail.ru
[2] tea471@mail.tsu.ru

Abstract. A finite Abelian p-group can be identified with a group $H = H_1 \oplus H_2 \oplus \ldots \oplus H_l$ with $H_i = \mathbf{Z}/p^{n_i}\mathbf{Z}$ and $n_1 \geq n_2 \geq \ldots \geq n_l = n > 0$. The endomorphisms of this group H are in one-to-one correspondence with the elements of the following set of matrices:

$$R = \begin{pmatrix} \mathbf{Z}/p^{n_1}\mathbf{Z} & \mathbf{Z}/p^{n_2}\mathbf{Z} & \ldots & \mathbf{Z}/p^{n_l}\mathbf{Z} \\ \mathbf{Z}/p^{n_2}\mathbf{Z} & \mathbf{Z}/p^{n_2}\mathbf{Z} & \ldots & \mathbf{Z}/p^{n_l}\mathbf{Z} \\ \ldots & \ldots & \ldots & \ldots \\ \mathbf{Z}/p^{n_l}\mathbf{Z} & \mathbf{Z}/p^{n_l}\mathbf{Z} & \ldots & \mathbf{Z}/p^{n_l}\mathbf{Z} \end{pmatrix}.$$

We endow R with a multiplication such that R becomes a ring which is isomorphic to the endomorphism ring End H of H. For $A \in R$, we define the determinant $|A| \in \mathbf{Z}/p^n\mathbf{Z}$ so that $|AA'| = |A| \cdot |A'|$. The main result is that the following are equivalent:
– The element $|A|$ is invertible in $\mathbf{Z}/p^n\mathbf{Z}$.
– The matrix A is left invertible in R.
– The matrix A is right invertible in R.
– The matrix A is invertible in R.
We also give an algorithm for finding A^{-1}.
Keywords: primary group, endomorphism ring, generalized matrix ring, inverse matrix

Acknowledgments: This work was supported by the Ministry of Science and Higher Education of Russia (agreement No. 075-02-2025-1728/2).

For citation: Stepanova, A.Yu., Timoshenko, E.A. (2025) Rings of generalized matrices representing endomorphisms of a finite primary group. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics*. 94. pp. 57–66. doi: 10.17223/19988621/94/5

Кольца обобщенных, или формальных, матриц возникли в связи с понятием контекста Мориты (подробнее см.: [1, 2]). За последние десятилетия появилось немало работ о кольцах обобщенных матриц, среди которых особенно выделим книгу П. Крылова и А. Туганбаева [3]. В некоторых кольцах обобщенных матриц удается ввести понятие определителя (см.: [4, 5]); ряд идей из этих статей мы используем ниже.

Кольца обобщенных матриц часто возникают в процессе исследования колец эндоморфизмов прямых сумм абелевых групп и модулей. Ранее в работе [6] мы показали, как представлять обобщенными матрицами эндоморфизмы конечных примарных групп рангов 2 и 3; были также получены формулы для нахождения обратной матрицы. В настоящей статье будет построено аналогичное представление уже для эндоморфизмов конечных примарных групп произвольного ранга и указан алгоритм вычисления обратной матрицы для этого случая.

Все группы, встречающиеся в статье, абелевы. Через $\mathbf{Z}$ мы обозначаем кольцо (и группу) целых чисел; ■ – символ конца доказательства либо его отсутствия.

Хорошо известно, что если $m \geq n > 0$ и p – простое число, то:

1) элементы группы гомоморфизмов $\mathrm{Hom}(\mathbf{Z}/p^m\mathbf{Z}, \mathbf{Z}/p^n\mathbf{Z})$ находятся во взаимно однозначном соответствии с элементами группы $\mathbf{Z}/p^n\mathbf{Z}$ (сопоставляем смежный класс $a + p^n\mathbf{Z}$ гомоморфизму $\psi \in \mathrm{Hom}(\mathbf{Z}/p^m\mathbf{Z}, \mathbf{Z}/p^n\mathbf{Z})$ такому, что для любого $z \in \mathbf{Z}$ выполнено $\psi(z + p^m\mathbf{Z}) = az + p^n\mathbf{Z}$);

2) элементы группы гомоморфизмов $\mathrm{Hom}(\mathbf{Z}/p^n\mathbf{Z}, \mathbf{Z}/p^m\mathbf{Z})$ находятся во взаимно однозначном соответствии с элементами группы $\mathbf{Z}/p^n\mathbf{Z}$ (сопоставляем смежный класс $b + p^n\mathbf{Z}$ гомоморфизму $\psi \in \mathrm{Hom}(\mathbf{Z}/p^n\mathbf{Z}, \mathbf{Z}/p^m\mathbf{Z})$ такому, что для любого $z \in \mathbf{Z}$ выполнено $\psi(z + p^n\mathbf{Z}) = p^{m-n}bz + p^m\mathbf{Z}$).

Ясно, что обе указанные биекции представляют собой изоморфизмы групп.

Любую конечную p-группу ранга l можно отождествить с подходящей прямой суммой $H = H_1 \oplus H_2 \oplus \ldots \oplus H_l$, где $H_i = \mathbf{Z}/p^{n_i}\mathbf{Z}$ и $n_1 \geq n_2 \geq \ldots \geq n_l > 0$. Элементы такой группы H будем записывать как векторы вида

$$\left(z_k + p^{n_k}\mathbf{Z} \right)_{k=1}^{l}, \tag{1}$$

где $z_k \in \mathbf{Z}$ (удобно представлять себе такой вектор как вектор-столбец). Далее для $i, j, k \in \{1, 2, \ldots, l\}$ введём обозначения

$$T_{ij} = \begin{cases} 1, & \text{если } i \geq j, \\ p^{n_i - n_j}, & \text{если } i \leq j, \end{cases}$$

$$S_{ijk} = \begin{cases} 1, & \text{если } i \leq j \leq k, \\ p^{n_k - n_j}, & \text{если } i \leq k \leq j, \\ p^{n_j - n_i}, & \text{если } j \leq i \leq k, \\ p^{n_j - n_k}, & \text{если } j \leq k \leq i, \\ p^{n_i - n_j}, & \text{если } k \leq i \leq j, \\ 1, & \text{если } k \leq j \leq i. \end{cases}$$

Несложно видеть, что даже со знаками нестрогого неравенства эти определения являются корректными. Из сказанного ранее ясно, что эндоморфизмы группы H находятся во взаимно однозначном соответствии с элементами множества

$$R = \begin{pmatrix} \mathbf{Z}/p^{n_1}\mathbf{Z} & \mathbf{Z}/p^{n_2}\mathbf{Z} & \ldots & \mathbf{Z}/p^{n_l}\mathbf{Z} \\ \mathbf{Z}/p^{n_2}\mathbf{Z} & \mathbf{Z}/p^{n_2}\mathbf{Z} & \ldots & \mathbf{Z}/p^{n_l}\mathbf{Z} \\ \ldots & \ldots & \ldots & \ldots \\ \mathbf{Z}/p^{n_l}\mathbf{Z} & \mathbf{Z}/p^{n_l}\mathbf{Z} & \ldots & \mathbf{Z}/p^{n_l}\mathbf{Z} \end{pmatrix},$$

состоящего из обобщенных матриц вида

$$A = \begin{pmatrix} a_{11} + p^{n_1}\mathbf{Z} & a_{12} + p^{n_2}\mathbf{Z} & \ldots & a_{1l} + p^{n_l}\mathbf{Z} \\ a_{21} + p^{n_2}\mathbf{Z} & a_{22} + p^{n_2}\mathbf{Z} & \ldots & a_{2l} + p^{n_l}\mathbf{Z} \\ \ldots & \ldots & \ldots & \ldots \\ a_{l1} + p^{n_l}\mathbf{Z} & a_{l2} + p^{n_l}\mathbf{Z} & \ldots & a_{ll} + p^{n_l}\mathbf{Z} \end{pmatrix} = \left(a_{ij} + p^{\min(n_i, n_j)}\mathbf{Z}\right)_{i,j=1}^{l} \qquad (2)$$

таких, что $a_{ij} \in \mathbf{Z}$. При этом эндоморфизму φ группы H мы сопоставляем матрицу вида (2) с тем свойством, что φ переводит всякий вектор вида (1) в вектор

$$\left(\sum_{k=1}^{l} T_{jk} a_{jk} z_k + p^{n_j}\mathbf{Z}\right)_{j=1}^{l}.$$

Ясно, что указанное соответствие:

– является групповым изоморфизмом;

– сопоставляет тождественному эндоморфизму группы H матрицу

$$E = \begin{pmatrix} 1 + p^{n_1}\mathbf{Z} & 0 + p^{n_2}\mathbf{Z} & \ldots & 0 + p^{n_l}\mathbf{Z} \\ 0 + p^{n_2}\mathbf{Z} & 1 + p^{n_2}\mathbf{Z} & \ldots & 0 + p^{n_l}\mathbf{Z} \\ \ldots & \ldots & \ldots & \ldots \\ 0 + p^{n_l}\mathbf{Z} & 0 + p^{n_l}\mathbf{Z} & \ldots & 1 + p^{n_l}\mathbf{Z} \end{pmatrix} = \left(\delta_{ij} + p^{\min(n_i, n_j)}\mathbf{Z}\right)_{i,j=1}^{l}, \qquad (3)$$

где δ_{ij} – символ Кронекера.

Установим некоторые свойства коэффициентов T_{ij} и S_{ijk}:

Лемма 1. а) Для любых $i, j, k \in \{1, 2, \ldots, l\}$ выполнено $T_{ik} S_{ijk} = T_{ij} T_{jk}$ и $S_{kji} = S_{ijk}$.

б) Для любых $i, j \in \{1, 2, \ldots, l\}$ выполнено $T_{ij} = S_{ij1}$ и $S_{iij} = S_{ijj} = 1$.

Доказательство. а) Достаточно рассмотреть шесть возможных случаев:

– если $i \le j \le k$, то $T_{ik}S_{ijk} = p^{n_i-n_k}\cdot 1 = p^{n_i-n_j}\cdot p^{n_j-n_k} = T_{ij}T_{jk}$ и $S_{kji} = 1$,

– если $i \le k \le j$, то $T_{ik}S_{ijk} = p^{n_i-n_k}\cdot p^{n_k-n_j} = p^{n_i-n_j}\cdot 1 = T_{ij}T_{jk}$ и $S_{kji} = p^{n_k-n_j}$,

– если $j \le i \le k$, то $T_{ik}S_{ijk} = p^{n_i-n_k}\cdot p^{n_j-n_i} = 1\cdot p^{n_j-n_k} = T_{ij}T_{jk}$ и $S_{kji} = p^{n_j-n_i}$,

– если $j \le k \le i$, то $T_{ik}S_{ijk} = 1\cdot p^{n_j-n_k} = T_{ij}T_{jk}$ и $S_{kji} = p^{n_j-n_k}$,

– если $k \le i \le j$, то $T_{ik}S_{ijk} = 1\cdot p^{n_i-n_j} = p^{n_i-n_j}\cdot 1 = T_{ij}T_{jk}$ и $S_{kji} = p^{n_i-n_j}$,

– если $k \le j \le i$, то $T_{ik}S_{ijk} = 1\cdot 1 = T_{ij}T_{jk}$ и $S_{kji} = 1$.

В каждом из этих случаев видим, что $S_{kji} = S_{ijk}$.

б) Непосредственно проверяется, что требуемые равенства верны как при $i \le j$, так и при $i \ge j$. ■

Заметим, что приведенные свойства в целом совпадают со свойствами систем множителей, с помощью которых можно задавать операцию умножения в кольце обобщенных матриц над некоторым кольцом с единицей (см.: [3, 4]).

Если эндоморфизму φ группы H соответствует матрица A, задаваемая равенством (2), а эндоморфизму φ′ – матрица

$$A' = \begin{pmatrix} a'_{11} + p^{n_1}\mathbf{Z} & a'_{12} + p^{n_2}\mathbf{Z} & \dots & a'_{1l} + p^{n_l}\mathbf{Z} \\ a'_{21} + p^{n_2}\mathbf{Z} & a'_{22} + p^{n_2}\mathbf{Z} & \dots & a'_{2l} + p^{n_l}\mathbf{Z} \\ \dots & \dots & \dots & \dots \\ a'_{l1} + p^{n_l}\mathbf{Z} & a'_{l2} + p^{n_l}\mathbf{Z} & \dots & a'_{ll} + p^{n_l}\mathbf{Z} \end{pmatrix}, \qquad (4)$$

то φ′ переводит всякий вектор вида (1) в вектор $\left(\sum_{k=1}^{l} T_{jk}a'_{jk}z_k + p^{n_j}\mathbf{Z}\right)_{j=1}^{l}$, поэтому φφ′ переводит (1) в вектор, равный

$$\left(\sum_{j=1}^{l} T_{ij}a_{ij}\sum_{k=1}^{l} T_{jk}a'_{jk}z_k + p^{n_i}\mathbf{Z}\right)_{i=1}^{l} = \left(\sum_{j=1}^{l}\sum_{k=1}^{l} T_{ij}T_{jk}a_{ij}a'_{jk}z_k + p^{n_i}\mathbf{Z}\right)_{i=1}^{l} =$$

$$= \left(\sum_{j=1}^{l}\sum_{k=1}^{l} T_{ik}S_{ijk}a_{ij}a'_{jk}z_k + p^{n_i}\mathbf{Z}\right)_{i=1}^{l} = \left(\sum_{k=1}^{l} T_{ik}\sum_{j=1}^{l} S_{ijk}a_{ij}a'_{jk}z_k + p^{n_i}\mathbf{Z}\right)_{i=1}^{l}$$

(здесь мы использовали лемму 1). Введем на множестве R операцию умножения, считая, что для матриц (2) и (4) выполнено

$$AA' = \left(\sum_{j=1}^{l} S_{ijk}a_{ij}a'_{jk} + p^{\min(n_i,n_k)}\mathbf{Z}\right)_{i,k=1}^{l}. \qquad (5)$$

Из наших рассуждений следует, что эта операция задана корректно и что верна

Теорема 2. Множество обобщенных матриц R с поэлементным сложением и операцией умножения, задаваемой равенством (5), образует кольцо, изоморфное кольцу эндоморфизмов End H группы H. Единичным элементом кольца R служит матрица (3). ■

Кольцо R в частном случае $n_i = l + 1 - i$ рассматривалось также в работе [7], где оно было использовано для построения криптосистемы.

Далее будем использовать обозначение $n = n_l$. Про целочисленную матрицу

$$X = \begin{pmatrix} T_{11}a_{11} & T_{12}a_{12} & \dots & T_{1l}a_{1l} \\ T_{21}a_{21} & T_{22}a_{22} & \dots & T_{2l}a_{2l} \\ \dots & \dots & \dots & \dots \\ T_{l1}a_{l1} & T_{l2}a_{l2} & \dots & T_{ll}a_{ll} \end{pmatrix} = \left(T_{ij}a_{ij}\right)_{i,j=1}^{l} \tag{6}$$

будем говорить, что она *порождает* матрицу (2); ясно, что для всякой матрицы $A \in R$ существует бесконечно много порождающих целочисленных матриц. Если

$$X' = \begin{pmatrix} T_{11}a'_{11} & T_{12}a'_{12} & \dots & T_{1l}a'_{1l} \\ T_{21}a'_{21} & T_{22}a'_{22} & \dots & T_{2l}a'_{2l} \\ \dots & \dots & \dots & \dots \\ T_{l1}a'_{l1} & T_{l2}a'_{l2} & \dots & T_{ll}a'_{ll} \end{pmatrix} = \left(T_{ij}a'_{ij}\right)_{i,j=1}^{l} \tag{7}$$

есть еще одна порождающая матрица для (2), то $a'_{ij} \equiv a_{ij} \pmod{p^n}$ для любых i и j, отсюда $T_{ij}a'_{ij} \equiv T_{ij}a_{ij} \pmod{p^n}$ и, значит, $\det X' \equiv \det X \pmod{p^n}$, где символ det обозначает обычный определитель. Это позволяет нам дать следующее

Определение 3. *Определителем* матрицы $A \in R$, заданной соотношением (2), назовем смежный класс $|A| = \det X + p^n\mathbf{Z}$, где X есть произвольная целочисленная матрица, порождающая матрицу A.

Так как E порождается единичной целочисленной матрицей, то $|E| = 1 + p^n\mathbf{Z}$.

Теорема 4. Для любых $A, A' \in R$ выполнено $|AA'| = |A| \cdot |A'|$.

Доказательство. Пусть матрицы A и A' заданы равенствами (2) и (4). Задавая X и X' равенствами (6) и (7), с учетом леммы 1 имеем

$$XX' = \left(\sum_{j=1}^{l}(T_{ij}a_{ij})(T_{jk}a'_{jk})\right)_{i,k=1}^{l} = \left(T_{ik}\sum_{j=1}^{l}S_{ijk}a_{ij}a'_{jk}\right)_{i,k=1}^{l}.$$

Сопоставляя эти равенства с записью (5), видим, что матрица XX' порождает AA', а значит,

$$|AA'| = \det(XX') + p^n\mathbf{Z} = (\det X + p^n\mathbf{Z})(\det X' + p^n\mathbf{Z}) = |A| \cdot |A'|,$$

что и требовалось. ■

Из следующего известного факта вытекает, что в кольце R обратимость обобщенной матрицы слева (или справа) эквивалентна ее двусторонней обратимости:

Предложение 5. В конечном кольце с единицей каждый левый (или правый) обратный элемент является также двусторонним обратным. ■

Если $n_1 = n$, то R – это множество всех матриц порядка l над $\mathbf{Z}/p^n\mathbf{Z}$. При этом для всех $i, j, k \in \{1, 2, \dots, l\}$ выполнено $S_{ijk} = T_{ij} = 1$, а значит, операция умножения и определитель в R будут совпадать с обычными; поэтому вопрос об обратимости матриц решается стандартным образом в соответствии с теоремой 6:

Теорема 6 [8]. а) В кольце Γ_l матриц порядка l над коммутативным кольцом с единицей Γ для всякой матрицы A выполнено

$$AA^* = A^*A = \left(\delta_{ij} \cdot \det A\right)_{i,\,j=1}^{l},$$

где A^* – союзная матрица.

б) Матрица A обратима в Γ_l тогда и только тогда, когда ее определитель $\det A$ обратим в Γ. Обратная матрица в этом случае имеет вид: $A^{-1} = (\det A)^{-1} \cdot A^*$. ■

Если $n_1 > n$, то существует число s такое, что $n_s > n_{s+1} = n$. Пусть матрица $A \in R$ задана соотношением (2). Мы будем разбивать матрицы из R и порождающие их целочисленные матрицы на блоки, левый верхний из которых имеет размер $s \times s$:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix},\ X = \begin{pmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{pmatrix}. \tag{8}$$

Всякая обобщенная матрица вида A_{11} представляет подходящий эндоморфизм прямой суммы $H_1 \oplus H_2 \oplus \ldots \oplus H_s$. Умножение в кольце R_s всех таких обобщенных матриц, изоморфном $\mathrm{End}(H_1 \oplus H_2 \oplus \ldots \oplus H_s)$, задается с помощью той же системы множителей S_{ijk}, что и в R (с ограничением $i, j, k \in \{1, 2, \ldots, s\}$).

Единичный элемент кольца R_s, который совпадает с левым верхним блоком матрицы (3), обозначим через E_s; далее через E_{l-s} будем обозначать единичную матрицу порядка $l - s$ над кольцом $\mathbf{Z}/p^n\mathbf{Z}$. Если $A_{12} = 0$ или $A_{21} = 0$, то

$$\begin{pmatrix} E_s & A_{12} \\ A_{21} & E_{l-s} \end{pmatrix}\begin{pmatrix} E_s & -A_{12} \\ -A_{21} & E_{l-s} \end{pmatrix} = \left(E + \begin{pmatrix} 0 & A_{12} \\ A_{21} & 0 \end{pmatrix}\right)\left(E - \begin{pmatrix} 0 & A_{12} \\ A_{21} & 0 \end{pmatrix}\right) =$$

$$= E - \begin{pmatrix} 0 & A_{12} \\ A_{21} & 0 \end{pmatrix} + \begin{pmatrix} 0 & A_{12} \\ A_{21} & 0 \end{pmatrix} - \begin{pmatrix} 0 & A_{12} \\ A_{21} & 0 \end{pmatrix}^2 = E\,. \tag{9}$$

Следующий результат является ключевым для установления критерия обратимости матриц из кольца R и, по сути, содержит алгоритм нахождения обратной матрицы. При построении этого алгоритма существенно используются формулы, которые позволяют строить обратную матрицу в кольце обобщенных матриц над некоторым коммутативным кольцом с единицей (см. [3, 4]).

Теорема 7. Пусть матрица $A \in R$ вида (2) такова, что ее блок A_{11} обратим в R_s. Если при этом для матрицы (6), порождающей A, выполнено условие $\det X \notin p\mathbf{Z}$, то матрица A обратима в R.

Доказательство. Пусть $X = (x_{ij})_{i,\,j=1}^{l}$ и A_{11}^{-1} – элемент кольца R_s, обратный к матрице A_{11}. Рассмотрим матрицу

$$U = \begin{pmatrix} A_{11}^{-1} & 0 \\ B_{21} & B_{22} \end{pmatrix} \in R\,,$$

у которой при $i > s$ на пересечении i-й строки и j-го столбца находится смежный класс $b_{ij} + p^n\mathbf{Z} = (\det X + p^n\mathbf{Z})^{-1} \cdot (X_{ji} + p^n\mathbf{Z})$, где через X_{ji}, как обычно, обозначено алгебраическое дополнение элемента x_{ji} матрицы X.

Пусть $i > s$. Тогда для любых j и k выполняется $T_{ij} = T_{ik} = 1$, откуда по лемме 1 получаем $S_{ijk} = T_{jk}$. Учитывая утверждение а) из теоремы 6, мы можем заключить, что для любого k справедливы равенства

$$\sum_{j=1}^{l} S_{ijk} X_{ji} a_{jk} = \sum_{j=1}^{l} X_{ji}(T_{jk} a_{jk}) = \sum_{j=1}^{l} X_{ji} x_{jk} = \delta_{ik} \cdot \det X$$

и, следовательно,

$$\sum_{j=1}^{l} S_{ijk} b_{ij} a_{jk} + p^n \mathbf{Z} = (\det X + p^n \mathbf{Z})^{-1} \cdot \left(\sum_{j=1}^{l} S_{ijk} X_{ji} a_{jk} + p^n \mathbf{Z} \right) =$$

$$= (\det X + p^n \mathbf{Z})^{-1} \cdot (\delta_{ik} + p^n \mathbf{Z})(\det X + p^n \mathbf{Z}) = \delta_{ik} + p^n \mathbf{Z} .$$

Отсюда вытекает, что матрица UA является блочно-унитреугольной:

$$UA = \begin{pmatrix} A_{11}^{-1} & 0 \\ B_{21} & B_{22} \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \begin{pmatrix} E_s & * \\ 0 & E_{l-s} \end{pmatrix}.$$

Учитывая (9), получаем, что для A существует левая обратная матрица, которая имеет вид:

$$(UA)^{-1} U = \begin{pmatrix} E_s & * \\ 0 & E_{l-s} \end{pmatrix} U = \left(E + \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \right) U = \begin{pmatrix} * & * \\ B_{21} & B_{22} \end{pmatrix}.$$

Рассмотрим теперь алгебраическое дополнение X_{ji} элемента x_{ji} матрицы X для случая $i \le s < j$. Всякое входящее в X_{ji} слагаемое содержит множитель, имеющий вид: $x_{ii_1} x_{i_1 i_2} \ldots x_{i_{t-1} i_t} x_{i_t j}$, где $t \ge 0$ и $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, l\}$. Ввиду леммы 1 из этого следует, что каждое такое слагаемое будет содержать множитель, равный

$$T_{ii_1} T_{i_1 i_2} \ldots T_{i_{t-1} i_t} T_{i_t j} = S_{ii_1 i_2} T_{ii_2} T_{i_2 i_3} \ldots T_{i_{t-1} i_t} T_{i_t j} = S_{ii_1 i_2} S_{ii_2 i_3} T_{ii_3} \ldots T_{i_{t-1} i_t} T_{i_t j} =$$

$$= S_{ii_1 i_2} S_{ii_2 i_3} \ldots S_{ii_{t-1} i_t} T_{ii_t} T_{i_t j} = S_{ii_1 i_2} S_{ii_2 i_3} \ldots S_{ii_{t-1} i_t} S_{ii_t j} T_{ij} .$$

Тем самым показано, что X_{ji} делится на T_{ij}; обозначим через Y_{ij} целое число, для которого $X_{ji} = T_{ij} Y_{ij}$. Чтобы последнее равенство выполнялось при $j > s$ для всех i, положим $Y_{ij} = X_{ji}$ при любых $i, j \in \{s+1, s+2, \ldots, l\}$. Рассмотрим матрицу

$$V = \begin{pmatrix} A_{11}^{-1} & B_{12} \\ 0 & B_{22} \end{pmatrix} \in R ,$$

у которой при $j > s$ на пересечении i-й строки и j-го столбца находится смежный класс $b_{ij} + p^n \mathbf{Z} = (\det X + p^n \mathbf{Z})^{-1} \cdot (Y_{ij} + p^n \mathbf{Z})$. Из определения Y_{ij} следует, что блок B_{22} в матрицах U и V – это действительно одна и та же матрица.

Для любых i и k выполняется $T_{ik} \delta_{ik} = \delta_{ik}$. Если $k > s$, то по лемме 1 и теореме 6 получаем, что для любого i справедливы равенства

$$T_{ik} \sum_{j=1}^{l} S_{ijk} a_{ij} Y_{jk} = \sum_{j=1}^{l} (T_{ij} a_{ij})(T_{jk} Y_{jk}) = \sum_{j=1}^{l} x_{ij} X_{kj} = \delta_{ik} \cdot \det X ,$$

отсюда $\sum_{j=1}^{l} S_{ijk} a_{ij} Y_{jk} = T_{ik}^{-1} \cdot \delta_{ik} \cdot \det X = \delta_{ik} \cdot \det X$ и, далее,

$$\sum_{j=1}^{l} S_{ijk} a_{ij} b_{jk} + p^n \mathbf{Z} = (\det X + p^n \mathbf{Z})^{-1} \cdot \left(\sum_{j=1}^{l} S_{ijk} a_{ij} Y_{jk} + p^n \mathbf{Z} \right) =$$

$$= (\det X + p^n \mathbf{Z})^{-1} \cdot (\delta_{ik} + p^n \mathbf{Z})(\det X + p^n \mathbf{Z}) = \delta_{ik} + p^n \mathbf{Z} .$$

Это означает, что матрица AV также является блочно-унитреугольной:

$$AV = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} A_{11}^{-1} & B_{12} \\ 0 & B_{22} \end{pmatrix} = \begin{pmatrix} E_s & 0 \\ * & E_{l-s} \end{pmatrix}.$$

С учетом (9) получаем, что для A существует правая обратная матрица, имеющая следующий вид:

$$V(AV)^{-1} = V\begin{pmatrix} E_s & 0 \\ * & E_{l-s} \end{pmatrix} = V\left(E + \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix}\right) = \begin{pmatrix} * & B_{12} \\ * & B_{22} \end{pmatrix}.$$

Из предложения 5 вытекает, что найденная правая обратная матрица обязательно совпадает с левой обратной, т.е.

$$A^{-1} = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix},\ A^{-1}\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = E = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} A^{-1}.$$

Выше показано, как можно найти блоки B_{12}, B_{21} и B_{22}, используя алгебраические дополнения к элементам матрицы X. Далее из соотношений

$$\begin{pmatrix} B_{11} & B_{12} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} A_{11} & 0 \\ A_{21} & 0 \end{pmatrix} = \begin{pmatrix} E_s & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} B_{11} & 0 \\ B_{21} & 0 \end{pmatrix}$$

легко выразить матрицы $B_{11}A_{11}$ и $A_{11}B_{11}$. Зная одну из этих матриц, можно найти блок B_{11}, воспользовавшись обратимостью матрицы $A_{11} \in R_s$. ■

Теперь мы готовы сформулировать и доказать критерий обратимости матриц в кольце R. Пусть m совпадает хотя бы с одним из чисел $n_1, n_2, \ldots, n_l$. Будем называть *диагональным m-блоком* матрицы $A \in R$ ту ее подматрицу, элементы которой находятся в A в позициях (i, j) таких, что $n_i = n_j = m$. Очевидно, что всякий m-блок представляет собой обычную квадратную матрицу над $\mathbf{Z}/p^m\mathbf{Z}$. Соответствующие подматрицы целочисленной матрицы X, порождающей A, тоже будем называть ее диагональными блоками (элементы $T_{ij}a_{ij}$ таких блоков – это просто числа a_{ij}).

Теорема 8. Пусть матрица $A \in R$ и порождающая ее целочисленная матрица X заданы равенствами (2) и (6) соответственно. Следующие условия эквивалентны:

1. Матрица A обратима в кольце R.
2. Элемент $|A|$ обратим в кольце $\mathbf{Z}/p^n\mathbf{Z}$.
3. Число $\det X \in \mathbf{Z}$ не делится на p.
4. Для всякого m диагональный m-блок матрицы A обратим в соответствующем матричном кольце.
5. Для всякого m определитель диагонального m-блока матрицы A обратим в кольце $\mathbf{Z}/p^m\mathbf{Z}$.
6. Определители всех диагональных блоков матрицы X не делятся на p.

Доказательство. Предположим, что эквивалентность перечисленных шести условий уже установлена для ситуации, когда матрицы из кольца R представляют эндоморфизмы p-группы ранга $< l$. Рассмотрим два случая.

I. Пусть $n_1 = n$. Как уже отмечено ранее, в этом случае R есть обычное кольцо квадратных матриц порядка l над $\mathbf{Z}/p^n\mathbf{Z}$. Ясно, что условия 4, 5 и 6 совпадают соответственно с условиями 1, 2 и 3. Наконец, условия 1 и 2 эквивалентны по теореме 6, а условия 2 и 3 – в силу равенства $|A| = \det X + p^n\mathbf{Z}$.

II. Пусть $n_1 > n$. Условия 4, 5 и 6 эквивалентны ввиду сказанного выше при рассмотрении случая I.

Импликация $1 \Rightarrow 2$ верна, так как для обратимой матрицы $A \in R$ выполнено $|A| \cdot |A^{-1}| = |AA^{-1}| = |E| = 1 + p^n\mathbf{Z}$.

Если элемент $|A|$ кольца $\mathbf{Z}/p^n\mathbf{Z}$ обратим, то из $|A| = \det X + p^n\mathbf{Z}$ получаем, что $\det X \notin p\mathbf{Z}$, т.е. импликация $2 \Rightarrow 3$ тоже справедлива.

Для завершения доказательства рассмотрим представление (8) матрицы X. Если $i \le s < j$, то $n_i > n_j$ и, следовательно, $T_{ij} \in p\mathbf{Z}$. Поэтому, разлагая определитель $\det X$ по первым s строкам в соответствии с теоремой Лапласа, приходим к сравнению $\det X \equiv \det W_{11} \cdot \det W_{22} \pmod p$. Это значит, что $\det X \notin p\mathbf{Z}$ тогда и только тогда, когда $\det W_{11} \notin p\mathbf{Z}$ и $\det W_{22} \notin p\mathbf{Z}$. Применяя к матрице W_{11} предположение индукции, можем сделать вывод, что условие $\det W_{11} \notin p\mathbf{Z}$ равносильно тому, что определители всех диагональных блоков из W_{11} не делятся на число p. Тем самым мы показали, что условия 3 и 6 для матрицы X эквивалентны.

Остается доказать импликацию $3 \Rightarrow 1$. Как мы уже знаем, из условия 3 следует, что определители всех диагональных блоков из W_{11} не делятся на p. В силу предположения индукции это означает, что порождаемая матрицей W_{11} матрица A_{11} обратима в R_s. По теореме 7 получаем, что матрица A обратима в R. ■

Матрица A^{-1} единственна (если она вообще существует). Отсюда, в частности, немедленно вытекает, что механизм построения A^{-1}, описанный в теоремах 7 и 8, приводит к одному и тому же результату вне зависимости от того, какая именно порождающая матрица X была выбрана для A.

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. *Крылов П.А., Туганбаев А.А.* Кольца формальных матриц и модули над ними. М.: МЦНМО, 2017.
4. *Крылов П.А., Туганбаев А.А.* Формальные матрицы и их определители // Фундаментальная и прикладная математика. 2014. № 1 (19). С. 65–119.
5. *Крылов П.А.* Определители обобщенных матриц порядка 2 // Фундаментальная и прикладная математика. 2015. № 5 (20). С. 95–112.
6. *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
7. *Climent J.-J., López-Ramos J.A.* Public key protocols over the ring $E_p^{(m)}$ // Adv. Math. Commun. 2016. V. 10 (4). P. 861–870. doi: 10.3934/amc.2016046
8. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. М.: Гелиос АРВ, 2003. Т. 1.

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. Krylov P., Tuganbaev A. (2017) *Formal Matrices*. (Algebra and Applications, Vol. 23). Springer. DOI: 10.1007/978-3-319-53907-2.
4. 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.
5. 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.
6. 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.

7. Climent J.-J., López-Ramos J.A. (2016) Public key protocols over the ring $E_p^{(m)}$. *Advances in Mathematics of Communications*. 10(4). pp. 861–870. DOI: 10.3934/amc.2016046.
8. Glukhov M.M., Elizarov V.P., Nechaev A.A. (2003) *Algebra* [Algebra]. Vol. 1. Moscow: Gelios ARV.

***Сведения об авторах*:**
Степанова Александра Юрьевна – аспирант механико-математического факультета Томского государственного университета (Томск, Россия). E-mail: stepanova.alexa@mail.ru
Тимошенко Егор Александрович – доктор физико-математических наук, доцент, ведущий научный сотрудник Регионального научно-образовательного математического центра Томского государственного университета, профессор кафедры алгебры механико-математического факультета Томского государственного университета (Томск, Россия). E-mail: tea471@mail.tsu.ru

***Information about the authors*:**
Stepanova Aleksandra Yu. (Tomsk State University, Tomsk, Russian Federation). E-mail: stepanova.alexa@mail.ru
Timoshenko Egor A. (Doctor of Physics and Mathematics, Tomsk State University, Tomsk, Russian Federation). E-mail: tea471@mail.tsu.ru

Статья поступила в редакцию 06.01.2025; принята к публикации 10.04.2025

The article was submitted 06.01.2025; accepted for publication 10.04.2025