УДК 512.541 MSC 16S50
DOI 10.17223/19988621/74/4

А.Ю. Степанова, Е.А. Тимошенко

МАТРИЧНОЕ ПРЕДСТАВЛЕНИЕ ЭНДОМОРФИЗМОВ ПРИМАРНЫХ ГРУПП МАЛЫХ РАНГОВ[1]

Для колец эндоморфизмов конечных примарных абелевых групп ранга 2 и 3 построены изоморфные им кольца обобщённых матриц. В каждом из этих матричных колец найдены необходимые и достаточные условия обратимости матриц, а также формулы для построения обратной матрицы.

Ключевые слова: *примарная группа, кольцо эндоморфизмов, кольцо обобщённых матриц, обратная матрица.*

Кольца обобщённых, или формальных, матриц берут начало в исследованиях Мориты (см. [1]). За последние десятилетия появилось много работ, посвящённых кольцам обобщённых матриц, а также модулям над ними; в первую очередь выделим монографию Крылова и Туганбаева [2]. Модули над кольцами обобщённых матриц порядка 2 и 3 рассматривались, в частности, в работах [3, 4]. В некоторых кольцах обобщённых матриц удаётся ввести понятие определителя матрицы (подробнее см. [5, 6]).

Кольца обобщённых матриц часто возникают при изучении колец эндоморфизмов прямых сумм абелевых групп и модулей. В данной статье представлены исследования колец эндоморфизмов конечных примарных групп ранга 2 и 3 и соответствующих им колец обобщённых матриц. Для таких матриц найдены критерии обратимости и формулы, позволяющие построить обратную матрицу.

Представление эндоморфизмов конечных *p*-групп ранга 2

Все группы, встречающиеся в статье, являются абелевыми. Через $\mathbf{Z}$ обозначается кольцо (и группа) целых чисел; ■ – символ конца доказательства либо его отсутствия.

Пусть p – простое число. Известно, что если $m \ge n > 0$, то:

1) элементы группы $\mathrm{Hom}(\mathbf{Z}/p^m\mathbf{Z}, \mathbf{Z}/p^n\mathbf{Z})$ находятся во взаимно однозначном соответствии с элементами группы $\mathbf{Z}/p^n\mathbf{Z}$ (элемент $a+p^n\mathbf{Z}$ сопоставляется гомоморфизму $\psi \in \mathrm{Hom}(\mathbf{Z}/p^m\mathbf{Z}, \mathbf{Z}/p^n\mathbf{Z})$, такому, что $\psi(z+p^m\mathbf{Z}) = az+p^n\mathbf{Z}$ при всех $z \in \mathbf{Z}$);

2) элементы группы $\mathrm{Hom}(\mathbf{Z}/p^n\mathbf{Z}, \mathbf{Z}/p^m\mathbf{Z})$ находятся во взаимно однозначном соответствии с элементами группы $\mathbf{Z}/p^n\mathbf{Z}$ (элемент $b+p^n\mathbf{Z}$ сопоставляется гомоморфизму $\psi \in \mathrm{Hom}(\mathbf{Z}/p^n\mathbf{Z}, \mathbf{Z}/p^m\mathbf{Z})$, такому, что $\psi(z+p^n\mathbf{Z}) = p^{m-n}bz+p^m\mathbf{Z}$ при всех z).

Заметим, что в каждом из двух случаев указанная биекция представляет собой групповой изоморфизм.

Всякая конечная p-группа H ранга 2 может быть отождествлена с подходящей группой вида $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z})$, где $m \ge n > 0$; её элементы будем записывать как

[1] Работа выполнена при поддержке Министерства науки и высшего образования РФ (соглашение № 075-02-2021-1392).

вектор-столбцы. Из сказанного выше следует, что эндоморфизмы группы H находятся во взаимно однозначном соответствии с элементами множества

$$R_2 = \begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \end{pmatrix},$$

состоящего из обобщённых матриц вида

$$A = \begin{pmatrix} a + p^m\mathbf{Z} & b + p^n\mathbf{Z} \\ c + p^n\mathbf{Z} & d + p^n\mathbf{Z} \end{pmatrix}, \tag{1}$$

где $a, b, c, d \in \mathbf{Z}$. При этом эндоморфизму φ группы H сопоставляется та единственная матрица вида (1), для которой при любых $z_1, z_2 \in \mathbf{Z}$ выполнено

$$\varphi\begin{pmatrix} z_1 + p^m\mathbf{Z} \\ z_2 + p^n\mathbf{Z} \end{pmatrix} = \begin{pmatrix} az_1 + p^{m-n}bz_2 + p^m\mathbf{Z} \\ cz_1 + dz_2 + p^n\mathbf{Z} \end{pmatrix}.$$

Ясно, что указанное соответствие:

- является групповым изоморфизмом;
- сопоставляет тождественному эндоморфизму группы H матрицу

$$E = \begin{pmatrix} 1 + p^m\mathbf{Z} & 0 + p^n\mathbf{Z} \\ 0 + p^n\mathbf{Z} & 1 + p^n\mathbf{Z} \end{pmatrix}. \tag{2}$$

Пусть эндоморфизму φ' группы H соответствует матрица

$$A' = \begin{pmatrix} a' + p^m\mathbf{Z} & b' + p^n\mathbf{Z} \\ c' + p^n\mathbf{Z} & d' + p^n\mathbf{Z} \end{pmatrix}. \tag{3}$$

Тогда для любых целых чисел z_1 и z_2 выполнено

$$(\varphi\varphi')\begin{pmatrix} z_1 + p^m\mathbf{Z} \\ z_2 + p^n\mathbf{Z} \end{pmatrix} = \varphi\begin{pmatrix} a'z_1 + p^{m-n}b'z_2 + p^m\mathbf{Z} \\ c'z_1 + d'z_2 + p^n\mathbf{Z} \end{pmatrix} =$$

$$= \begin{pmatrix} aa'z_1 + p^{m-n}ab'z_2 + p^{m-n}bc'z_1 + p^{m-n}bd'z_2 + p^m\mathbf{Z} \\ ca'z_1 + p^{m-n}cb'z_2 + dc'z_1 + dd'z_2 + p^n\mathbf{Z} \end{pmatrix} =$$

$$= \begin{pmatrix} (aa' + p^{m-n}bc')z_1 + p^{m-n}(ab' + bd')z_2 + p^m\mathbf{Z} \\ (ca' + dc')z_1 + (p^{m-n}cb' + dd')z_2 + p^n\mathbf{Z} \end{pmatrix}.$$

Введём на R_2 операцию умножения, считая, что для матриц (1) и (3) выполнено

$$AA' = \begin{pmatrix} aa' + p^{m-n}bc' + p^m\mathbf{Z} & ab' + bd' + p^n\mathbf{Z} \\ ca' + dc' + p^n\mathbf{Z} & p^{m-n}cb' + dd' + p^n\mathbf{Z} \end{pmatrix}. \tag{4}$$

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

Теорема 1. Множество обобщённых матриц R_2 с поэлементным сложением и операцией умножения, задаваемой равенством (4), образует кольцо, изоморфное кольцу эндоморфизмов End H группы H. Единичным элементом кольца R_2 служит матрица (2). ■

Кольцо R_2 для случая $m > n$ рассматривалось также в [2, 5, 6].

Определителем матрицы $A \in R_2$ вида (1) назовём элемент $|A| = ad - p^{m-n}bc + p^n\mathbf{Z}$ кольца $\mathbf{Z}/p^n\mathbf{Z}$.

Если для матриц (1) и (3) выполнено $A = A'$, то в силу неравенства $m \geq n$ будут справедливы следующие сравнения по модулю p^n:

$$a \equiv a',\ b \equiv b',\ c \equiv c',\ d \equiv d',\ ad - p^{m-n}bc \equiv a'd' - p^{m-n}b'c'.$$

Значит, понятие определителя введено корректно. Ясно также, что $|E| = 1 + p^n\mathbf{Z}$.

Предложение 2. Для любых $A, A' \in R_2$ выполнено $|AA'| = |A| \cdot |A'|$.

Доказательство. Действительно, для матрицы (4) имеем

$$\begin{aligned}|AA'| &= (aa' + p^{m-n}bc')(p^{m-n}cb' + dd') - p^{m-n}(ab' + bd')(ca' + dc') + p^n\mathbf{Z} = \\ &= aa'dd' + p^{m-n}aa'cb' + p^{m-n}bc'dd' + p^{2(m-n)}bc'cb' - \\ &- p^{m-n}ab'ca' - p^{m-n}ab'dc' - p^{m-n}bd'ca' - p^{m-n}bd'dc' + p^n\mathbf{Z} = \\ &= aa'dd' - p^{m-n}(ab'dc' + bd'ca') + p^{2(m-n)}bc'cb' + p^n\mathbf{Z} = \\ &= (ad - p^{m-n}bc)(a'd' - p^{m-n}b'c') + p^n\mathbf{Z} = |A| \cdot |A'|,\end{aligned}$$

что и требовалось. ■

Если $m = n$, то R_2 – это кольцо матриц, элементы которых принадлежат одному и тому же кольцу вычетов $\mathbf{Z}/p^n\mathbf{Z}$. В этом случае операция умножения и определитель в кольце R_2 совпадают с обычными; поэтому вопрос об обратимости матриц решается стандартным образом в соответствии со следующей теоремой (через K_l в ней обозначено кольцо $(l \times l)$-матриц над коммутативным кольцом K, содержащим единицу):

Теорема 3 [7]. Матрица $A = (a_{ij}) \in K_l$ обратима в K_l тогда и только тогда, когда её определитель $\det A$ обратим в кольце K. Если это условие выполнено, то обратная к A матрица имеет вид $A^{-1} = (\det A)^{-1} \cdot A^*$, где

$$A^* = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{l1} \\ A_{12} & A_{22} & \dots & A_{l2} \\ \dots & \dots & \dots & \dots \\ A_{1l} & A_{2l} & \dots & A_{ll} \end{pmatrix}$$

(через A_{ij} обозначено алгебраическое дополнение элемента a_{ij} матрицы A). ■

Таким образом, нам остаётся рассмотреть случай $m > n$.

Теорема 4. Пусть $m > n > 0$. Для матрицы $A \in R_2$ вида (1) равносильны следующие условия:

1) Числа a и d не делятся на p.
2) Элемент $|A|$ обратим в кольце $\mathbf{Z}/p^n\mathbf{Z}$.
3) Матрица A обратима слева в кольце R_2.
4) Матрица A обратима справа в кольце R_2.
5) Матрица A обратима в кольце R_2.

Если эти условия выполнены, то матрица A^{-1} находится по формуле

$$\begin{pmatrix} W(1 + p^{m-n}bcF) + p^m\mathbf{Z} & -bF + p^n\mathbf{Z} \\ -cF + p^n\mathbf{Z} & aF + p^n\mathbf{Z} \end{pmatrix}, \qquad (5)$$

где $F + p^n\mathbf{Z} = |A|^{-1} \in \mathbf{Z}/p^n\mathbf{Z}$ и $W + p^m\mathbf{Z} = (a + p^m\mathbf{Z})^{-1} \in \mathbf{Z}/p^m\mathbf{Z}$.

Доказательство. Импликация 5) $\Rightarrow$ 3) очевидна. Поскольку $m > n$, мы можем записать следующие эквивалентности:

$$|A| \text{ – обратимый элемент в } \mathbf{Z}/p^n\mathbf{Z} \Leftrightarrow \text{НОД}(ad - p^{m-n}bc, p) = 1 \Leftrightarrow$$

$$\Leftrightarrow \text{НОД}(ad, p) = 1 \Leftrightarrow \text{НОД}(a, p) = \text{НОД}(d, p) = 1.$$

Таким образом, условия 1) и 2) равносильны.

3) $\Rightarrow$ 2) и 4) $\Rightarrow$ 2). Если $B \in R_2$ – левая обратная или правая обратная матрица для A, то по предложению 2 имеем $|A| \cdot |B| = |E| = 1 + p^n\mathbf{Z}$. Таким образом, смежный класс $|B| \in \mathbf{Z}/p^n\mathbf{Z}$ является обратным элементом для смежного класса $|A|$.

2) $\Rightarrow$ 4). Пусть $|A|$ – обратимый элемент в $\mathbf{Z}/p^n\mathbf{Z}$. Так как справедлива импликация 2) $\Rightarrow$ 1), то число a не делится на p и, следовательно, элемент $a + p^m\mathbf{Z}$ обратим в кольце $\mathbf{Z}/p^m\mathbf{Z}$, т.е. существует элемент $W + p^m\mathbf{Z} = (a + p^m\mathbf{Z})^{-1}$. Поскольку $m > n$, то $aW + p^n\mathbf{Z} = 1 + p^n\mathbf{Z}$. Убедимся, что матрица B, задаваемая формулой (5), является правой обратной для матрицы A. Для элементов x_{ij} матрицы $X = AB$ имеем

$$x_{11} = aW(1 + p^{m-n}bcF) - p^{m-n}bcF + p^m\mathbf{Z} = aW + p^m\mathbf{Z} = 1 + p^m\mathbf{Z};$$

$$x_{12} = -abF + abF + p^n\mathbf{Z} = 0 + p^n\mathbf{Z};$$

$$x_{22} = -p^{m-n}bcF + adF + p^n\mathbf{Z} = (F + p^n\mathbf{Z})(ad - p^{m-n}bc + p^n\mathbf{Z}) = 1 + p^n\mathbf{Z};$$

$$\begin{aligned} x_{21} &= cW(1 + p^{m-n}bcF) - cdF + p^n\mathbf{Z} = cW(1 + p^{m-n}bcF) - cWadF + p^n\mathbf{Z} = \\ &= cW(1 + p^{m-n}bcF - adF) + p^n\mathbf{Z} = cW[(1 + p^n\mathbf{Z}) - x_{22}] = 0 + p^n\mathbf{Z}. \end{aligned}$$

Таким образом, $AB = E$, что и требовалось.

4) $\Rightarrow$ 5). Пусть $B \in R_2$ и $AB = E$. Так как справедлива импликация 3) $\Rightarrow$ 2), то смежный класс $|B|$ является обратимым элементом кольца $\mathbf{Z}/p^n\mathbf{Z}$. Пользуясь справедливостью импликации 2) $\Rightarrow$ 4), мы можем найти матрицу $B' \in R_2$, такую, что $BB' = E$. Тогда $A = AE = A(BB') = (AB)B' = EB' = B'$. Таким образом, $BA = E$, т.е. B – матрица, обратная к A. ■

В частности, мы получили, что обратимость матрицы $A \in R_2$ эквивалентна обратимости элемента $|A| \in \mathbf{Z}/p^n\mathbf{Z}$ как в случае $m = n$, так и в случае $m > n$ (что согласуется с результатами из [6]).

Замечание. Обратная матрица определена однозначно (если она существует). Отсюда, в частности, сразу следует, что задаваемая формулой (5) матрица не зависит от выбора конкретных чисел $a, b, c, d \in \mathbf{Z}$, удовлетворяющих равенству (1).

Представление эндоморфизмов конечных *p*-групп ранга 3

Перейдём к рассмотрению конечных p-групп ранга 3. Каждую такую группу H можно отождествить с группой вида $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z}) \oplus (\mathbf{Z}/p^k\mathbf{Z})$, где $m \geq n \geq k > 0$. Эндоморфизмы группы H находятся во взаимно однозначном соответствии с элементами множества

$$R_3 = \begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} \\ \mathbf{Z}/p^k\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} \end{pmatrix},$$

состоящего из обобщённых матриц вида

$$A = \begin{pmatrix} a_1 + p^m\mathbf{Z} & a_2 + p^n\mathbf{Z} & a_3 + p^k\mathbf{Z} \\ b_1 + p^n\mathbf{Z} & b_2 + p^n\mathbf{Z} & b_3 + p^k\mathbf{Z} \\ c_1 + p^k\mathbf{Z} & c_2 + p^k\mathbf{Z} & c_3 + p^k\mathbf{Z} \end{pmatrix}, \tag{6}$$

где $a_j, b_j, c_j \in \mathbf{Z}$. Эндоморфизму φ группы H сопоставляется та единственная матрица вида (6), для которой при любых $z_1, z_2, z_3 \in \mathbf{Z}$ выполнено

$$\varphi\begin{pmatrix} z_1 + p^m\mathbf{Z} \\ z_2 + p^n\mathbf{Z} \\ z_3 + p^k\mathbf{Z} \end{pmatrix} = \begin{pmatrix} a_1z_1 + p^{m-n}a_2z_2 + p^{m-k}a_3z_3 + p^m\mathbf{Z} \\ b_1z_1 + b_2z_2 + p^{n-k}b_3z_3 + p^n\mathbf{Z} \\ c_1z_1 + c_2z_2 + c_3z_3 + p^k\mathbf{Z} \end{pmatrix}.$$

Указанное соответствие является групповым изоморфизмом; ясно также, что оно сопоставляет тождественному эндоморфизму группы H матрицу

$$E=\begin{pmatrix} 1+p^m\mathbf{Z} & 0+p^n\mathbf{Z} & 0+p^k\mathbf{Z} \\ 0+p^n\mathbf{Z} & 1+p^n\mathbf{Z} & 0+p^k\mathbf{Z} \\ 0+p^k\mathbf{Z} & 0+p^k\mathbf{Z} & 1+p^k\mathbf{Z} \end{pmatrix}. \tag{7}$$

Пусть в дополнение к φ имеется эндоморфизм $\varphi' \in \operatorname{End} H$, которому соответствует матрица

$$A'=\begin{pmatrix} a_1'+p^m\mathbf{Z} & a_2'+p^n\mathbf{Z} & a_3'+p^k\mathbf{Z} \\ b_1'+p^n\mathbf{Z} & b_2'+p^n\mathbf{Z} & b_3'+p^k\mathbf{Z} \\ c_1'+p^k\mathbf{Z} & c_2'+p^k\mathbf{Z} & c_3'+p^k\mathbf{Z} \end{pmatrix}. \tag{8}$$

Непосредственные вычисления выражения

$$(\varphi\varphi')\begin{pmatrix} z_1+p^m\mathbf{Z} \\ z_2+p^n\mathbf{Z} \\ z_3+p^k\mathbf{Z} \end{pmatrix}=\varphi\begin{pmatrix} a_1'z_1+p^{m-n}a_2'z_2+p^{m-k}a_3'z_3+p^m\mathbf{Z} \\ b_1'z_1+b_2'z_2+p^{n-k}b_3'z_3+p^n\mathbf{Z} \\ c_1'z_1+c_2'z_2+c_3'z_3+p^k\mathbf{Z} \end{pmatrix},$$

где $z_1, z_2, z_3 \in \mathbf{Z}$, показывают, что эндоморфизму $\varphi\varphi'$ соответствует матрица

$$\begin{pmatrix} \overline{\overline{a_1a_1'+sa_2b_1'+sta_3c_1'}} & \overrightarrow{a_1a_2'+a_2b_2'+ta_3c_2'} & \overline{a_1a_3'+a_2b_3'+a_3c_3'} \\ \overrightarrow{b_1a_1'+b_2b_1'+tb_3c_1'} & \overrightarrow{sb_1a_2'+b_2b_2'+tb_3c_2'} & \overline{sb_1a_3'+b_2b_3'+b_3c_3'} \\ \overline{c_1a_1'+c_2b_1'+c_3c_1'} & \overline{sc_1a_2'+c_2b_2'+c_3c_2'} & \overline{stc_1a_3'+tc_2b_3'+c_3c_3'} \end{pmatrix}. \tag{9}$$

Здесь смежные классы $z+p^m\mathbf{Z}$, $z+p^n\mathbf{Z}$ и $z+p^k\mathbf{Z}$ обозначены через $\overline{\overline{z}}$, $\vec{z}$ и $\overline{z}$ соответственно, а через s и t для краткости обозначены множители p^{m-n} и p^{n-k}.

Введём на R_3 операцию умножения, считая, что произведение AA' матриц, заданных равенствами (6) и (8), равно матрице (9). Наши рассуждения показывают, что эта операция задана корректно и что имеет место

Теорема 5. Множество обобщённых матриц R_3 с поэлементным сложением и указанной выше операцией умножения представляет собой кольцо, изоморфное кольцу $\operatorname{End} H$. Единичным элементом кольца R_3 служит матрица (7). ■

Пусть матрица $A \in R_3$ имеет вид (6). Элемент

$$a_1b_2c_3-p^{n-k}a_1b_3c_2-p^{m-n}a_2b_1c_3+p^{m-k}(a_3b_1c_2+a_2b_3c_1-a_3b_2c_1)+p^k\mathbf{Z}$$

кольца $\mathbf{Z}/p^k\mathbf{Z}$ будем называть *определителем* матрицы A и обозначать через $|A|$. Как и в случае кольца R_2, из условия $m \geq n \geq k$ нетрудно вывести, что понятие определителя введено корректно. Заметим также, что $|E| = 1+p^k\mathbf{Z}$.

Предложение 6. Для любых $A, A' \in R_3$ выполнено $|AA'| = |A|\cdot|A'|$.

Доказательство. Пусть матрицы A и A' заданы равенствами (6) и (8). Легко видеть, что для целочисленных матриц

$$J=\begin{pmatrix} a_1 & sa_2 & sta_3 \\ b_1 & b_2 & tb_3 \\ c_1 & c_2 & c_3 \end{pmatrix},\quad J'=\begin{pmatrix} a_1' & sa_2' & sta_3' \\ b_1' & b_2' & tb_3' \\ c_1' & c_2' & c_3' \end{pmatrix}$$

справедливы равенства $|A| = \det J + p^k\mathbf{Z}$ и $|A'| = \det J' + p^k\mathbf{Z}$, где через $\det$ обозначен обычный определитель. Далее, сравнивая матрицу

$$\begin{pmatrix} a_1a_1' + sa_2b_1' + sta_3c_1' & s(a_1a_2' + a_2b_2' + ta_3c_2') & st(a_1a_3' + a_2b_3' + a_3c_3') \\ b_1a_1' + b_2b_1' + tb_3c_1' & sb_1a_2' + b_2b_2' + tb_3c_2' & t(sb_1a_3' + b_2b_3' + b_3c_3') \\ c_1a_1' + c_2b_1' + c_3c_1' & sc_1a_2' + c_2b_2' + c_3c_2' & stc_1a_3' + tc_2b_3' + c_3c_3' \end{pmatrix}$$

(которая, как нетрудно проверить, совпадает с обычным произведением JJ' матриц J и J') с матрицей (9), видим, что $|AA'| = \det(JJ') + p^k\mathbf{Z}$. Для завершения доказательства остаётся заметить, что $\det(JJ') = \det J \cdot \det J'$. ■

Следующий результат доказывается точно так же, как и справедливость импликаций 3) $\Rightarrow$ 2) и 4) $\Rightarrow$ 2) в теореме 4:

Лемма 7. Если матрица A обратима слева или справа в кольце R_3, то смежный класс $|A|$ является обратимым элементом кольца $\mathbf{Z}/p^k\mathbf{Z}$. ■

Критерии обратимости и формулы для обратных матриц в R_3 будем выводить поэтапно.

Лемма 8. Если определитель матрицы $A \in R_3$ вида (6) обратим в кольце $\mathbf{Z}/p^k\mathbf{Z}$ и матрица $B \in R_3$ имеет вид

$$\begin{pmatrix} * & * & F(a_2b_3 - a_3b_2) + p^k\mathbf{Z} \\ * & * & F(p^{m-n}a_3b_1 - a_1b_3) + p^k\mathbf{Z} \\ * & * & F(a_1b_2 - p^{m-n}a_2b_1) + p^k\mathbf{Z} \end{pmatrix}, \qquad (10)$$

где $F + p^k\mathbf{Z} = |A|^{-1} \in \mathbf{Z}/p^k\mathbf{Z}$, то третьи столбцы матриц AB и E совпадают.

Доказательство. Для элементов x_{i3} третьего столбца матрицы $X = AB$ имеем

$$\begin{gathered} x_{13} = a_1F(a_2b_3 - a_3b_2) + a_2F(p^{m-n}a_3b_1 - a_1b_3) + \\ + a_3F(a_1b_2 - p^{m-n}a_2b_1) + p^k\mathbf{Z} = F(a_1a_2b_3 - a_1b_2a_3 + \\ + p^{m-n}b_1a_2a_3 - a_1a_2b_3 + a_1b_2a_3 - p^{m-n}b_1a_2a_3) + p^k\mathbf{Z} = 0 + p^k\mathbf{Z}; \end{gathered}$$

$$\begin{gathered} x_{23} = p^{m-n}b_1F(a_2b_3 - a_3b_2) + b_2F(p^{m-n}a_3b_1 - a_1b_3) + \\ + b_3F(a_1b_2 - p^{m-n}a_2b_1) + p^k\mathbf{Z} = F(p^{m-n}b_1a_2b_3 - p^{m-n}b_1b_2a_3 + \\ + p^{m-n}b_1b_2a_3 - a_1b_2b_3 + a_1b_2b_3 - p^{m-n}b_1a_2b_3) + p^k\mathbf{Z} = 0 + p^k\mathbf{Z}; \end{gathered}$$

$$\begin{gathered} x_{33} = p^{m-k}c_1F(a_2b_3 - a_3b_2) + p^{n-k}c_2F(p^{m-n}a_3b_1 - a_1b_3) + \\ + c_3F(a_1b_2 - p^{m-n}a_2b_1) + p^k\mathbf{Z} = F[a_1b_2c_3 - p^{n-k}a_1b_3c_2 - p^{m-n}a_2b_1c_3 + \\ + p^{m-k}(a_2b_3c_1 - a_3b_2c_1 + a_3b_1c_2)] + p^k\mathbf{Z} = (F + p^k\mathbf{Z}) \cdot |A| = 1 + p^k\mathbf{Z}, \end{gathered}$$

что и требовалось. ■

Лемма 9. Если определитель матрицы $A \in R_3$ вида (6) обратим в кольце $\mathbf{Z}/p^k\mathbf{Z}$, разность $a_1b_2 - p^{m-n}a_2b_1$ не делится на p и матрица $B \in R_3$ имеет вид

$$\begin{pmatrix} * & -a_2Q + p^{n-k}a_3c_2F + p^n\mathbf{Z} & F(a_2b_3 - a_3b_2) + p^k\mathbf{Z} \\ * & a_1Q - p^{m-k}a_3c_1F + p^n\mathbf{Z} & F(p^{m-n}a_3b_1 - a_1b_3) + p^k\mathbf{Z} \\ * & F(p^{m-n}a_2c_1 - a_1c_2) + p^k\mathbf{Z} & F(a_1b_2 - p^{m-n}a_2b_1) + p^k\mathbf{Z} \end{pmatrix}, \qquad (11)$$

где целые числа F и Q задаются условиями

$$F + p^k\mathbf{Z} = |A|^{-1} \in \mathbf{Z}/p^k\mathbf{Z},\ G + p^n\mathbf{Z} = (a_1b_2 - p^{m-n}a_2b_1 + p^n\mathbf{Z})^{-1} \in \mathbf{Z}/p^n\mathbf{Z},$$

$$M = a_1b_3c_2 + p^{m-n}(a_3b_2c_1 - a_3b_1c_2 - a_2b_3c_1),\ Q = G(1 + p^{n-k}FM),$$

то у матриц AB и E совпадают второй и третий столбцы.

Доказательство. Заметим, что $|A| = a_1b_2c_3 - p^{m-n}a_2b_1c_3 - p^{n-k}M + p^k\mathbf{Z}$. Поскольку $n \ge k$, то справедливо равенство $G(a_1b_2 - p^{m-n}a_2b_1) + p^k\mathbf{Z} = 1 + p^k\mathbf{Z}$. Для элементов x_{i2} второго столбца матрицы $X = AB$ имеем

$$x_{12}=a_1(-a_2Q+p^{n-k}a_3c_2F)+a_2(a_1Q-p^{m-k}a_3c_1F)+$$
$$+p^{n-k}a_3F(p^{m-n}a_2c_1-a_1c_2)+p^n\mathbf{Z}=p^{n-k}a_1c_2a_3F-p^{m-k}c_1a_2a_3F+$$
$$+p^{n-k}F(p^{m-n}c_1a_2a_3-a_1c_2a_3)+p^n\mathbf{Z}=0+p^n\mathbf{Z};$$
$$x_{22}=p^{m-n}b_1(-a_2Q+p^{n-k}a_3c_2F)+b_2(a_1Q-p^{m-k}a_3c_1F)+$$
$$+p^{n-k}b_3F(p^{m-n}a_2c_1-a_1c_2)+p^n\mathbf{Z}=-p^{m-n}a_2b_1G(1+p^{n-k}FM)+$$
$$+p^{m-k}a_3b_1c_2F+a_1b_2G(1+p^{n-k}FM)-p^{m-k}a_3b_2c_1F+$$
$$+p^{n-k}F(p^{m-n}a_2b_3c_1-a_1b_3c_2)+p^n\mathbf{Z}=G(a_1b_2-p^{m-n}a_2b_1)(1+p^{n-k}FM)+$$
$$+p^{n-k}F(p^{m-n}a_3b_1c_2-p^{m-n}a_3b_2c_1+p^{m-n}a_2b_3c_1-a_1b_3c_2)+p^n\mathbf{Z}=$$
$$=1+p^{n-k}FM-p^{n-k}FM+p^n\mathbf{Z}=1+p^n\mathbf{Z};$$
$$x_{32}=p^{m-n}c_1(-a_2Q+p^{n-k}a_3c_2F)+c_2(a_1Q-p^{m-k}a_3c_1F)+$$
$$+c_3F(p^{m-n}a_2c_1-a_1c_2)+p^k\mathbf{Z}=-p^{m-n}a_2c_1G(1+p^{n-k}FM)+p^{m-k}c_1c_2a_3F+$$
$$+a_1c_2G(1+p^{n-k}FM)-p^{m-k}c_1c_2a_3F+c_3F(p^{m-n}a_2c_1-a_1c_2)+p^k\mathbf{Z}=$$
$$=(a_1c_2-p^{m-n}a_2c_1)G(1+p^{n-k}FM)+c_3F(p^{m-n}a_2c_1-a_1c_2)+p^k\mathbf{Z}=$$
$$=(a_1c_2-p^{m-n}a_2c_1)[G(1+p^{n-k}FM)-c_3F]+p^k\mathbf{Z}=$$
$$=(a_1c_2-p^{m-n}a_2c_1)G[1+p^{n-k}FM-(a_1b_2-p^{m-n}a_2b_1)c_3F]+p^k\mathbf{Z}=$$
$$=(a_1c_2-p^{m-n}a_2c_1)G[1+F(p^{n-k}M-a_1b_2c_3+p^{m-n}a_2b_1c_3)]+p^k\mathbf{Z}=$$
$$=(a_1c_2-p^{m-n}a_2c_1)G[(1+p^k\mathbf{Z})-(F+p^k\mathbf{Z})\cdot|A|]=0+p^k\mathbf{Z}.$$

Ввиду леммы 8 отсюда следует требуемое утверждение. ■

Следствие 10. Пусть $m=n\geq k>0$. Если определитель матрицы $A\in R_3$ вида (6) обратим в $\mathbf{Z}/p^k\mathbf{Z}$, разность $a_1b_2-a_2b_1$ не делится на p и матрица $B\in R_3$ имеет вид

$$\begin{pmatrix} * & -a_2Q+p^{n-k}a_3c_2F+p^n\mathbf{Z} & F(a_2b_3-a_3b_2)+p^k\mathbf{Z} \\ * & a_1Q-p^{n-k}a_3c_1F+p^n\mathbf{Z} & F(a_3b_1-a_1b_3)+p^k\mathbf{Z} \\ * & F(a_2c_1-a_1c_2)+p^k\mathbf{Z} & F(a_1b_2-a_2b_1)+p^k\mathbf{Z} \end{pmatrix}, \qquad (12)$$

где целые числа F и Q задаются условиями

$$F+p^k\mathbf{Z}=|A|^{-1}\in\mathbf{Z}/p^k\mathbf{Z},\ G+p^n\mathbf{Z}=(a_1b_2-a_2b_1+p^n\mathbf{Z})^{-1}\in\mathbf{Z}/p^n\mathbf{Z},$$
$$M=a_1b_3c_2+a_3b_2c_1-a_3b_1c_2-a_2b_3c_1,\ Q=G(1+p^{n-k}FM),$$

то у матриц AB и E совпадают второй и третий столбцы.

Доказательство. Требуемое утверждение следует из леммы 9 ввиду того факта, что при $m=n$ второй и третий столбцы матрицы (12) совпадают со вторым и третьим столбцами матрицы (11). ■

Теорема 11. Пусть $m=n>k>0$. Для матрицы $A\in R_3$ вида (6) равносильны следующие условия:

1) Числа $a_1b_2-a_2b_1$ и c_3 не делятся на p.

2) Элемент $|A|$ обратим в кольце $\mathbf{Z}/p^k\mathbf{Z}$.

3) Матрица A обратима слева в кольце R_3.

4) Матрица A обратима справа в кольце R_3.

5) Матрица A обратима в кольце R_3.

Если эти условия выполнены, то матрица A^{-1} имеет вид

$$\begin{pmatrix} b_2Q-p^{n-k}b_3c_2F+p^n\mathbf{Z} & * & * \\ -b_1Q+p^{n-k}b_3c_1F+p^n\mathbf{Z} & * & * \\ F(b_1c_2-b_2c_1)+p^k\mathbf{Z} & * & * \end{pmatrix}, \qquad (13)$$

где второй и третий столбцы берутся из матрицы (12), а целые числа F и Q задаются условиями

$$F+p^k\mathbf{Z}=|A|^{-1}\in\mathbf{Z}/p^k\mathbf{Z},\ G+p^n\mathbf{Z}=(a_1b_2-a_2b_1+p^n\mathbf{Z})^{-1}\in\mathbf{Z}/p^n\mathbf{Z},$$

$$M=a_1b_3c_2+a_3b_2c_1-a_3b_1c_2-a_2b_3c_1,\ Q=G(1+p^{n-k}FM).$$

Доказательство. Импликация 5) $\Rightarrow$ 3) очевидна; импликация 3) $\Rightarrow$ 2) верна в силу леммы 7.

Далее, так как $m=n$, то справедливо равенство

$$|A|=a_1b_2c_3-a_2b_1c_3+p^{n-k}(a_3b_1c_2+a_2b_3c_1-a_3b_2c_1-a_1b_3c_2)+p^k\mathbf{Z}.$$

Поскольку $n>k$, мы можем записать следующие эквивалентности:

$$|A| \text{ – обратимый элемент в } \mathbf{Z}/p^k\mathbf{Z} \Leftrightarrow \text{НОД}(a_1b_2c_3-a_2b_1c_3,p)=1 \Leftrightarrow$$

$$\Leftrightarrow \text{НОД}(a_1b_2-a_2b_1,p)=\text{НОД}(c_3,p)=1.$$

Таким образом, условия 1) и 2) равносильны.

2) $\Rightarrow$ 4). Пусть $|A|$ – обратимый элемент в $\mathbf{Z}/p^k\mathbf{Z}$. Так как справедлива импликация 2) $\Rightarrow$ 1), то смежный класс $a_1b_2-a_2b_1+p^n\mathbf{Z}$ обратим в $\mathbf{Z}/p^n\mathbf{Z}$, т.е. существует элемент $G+p^n\mathbf{Z}=(a_1b_2-a_2b_1+p^n\mathbf{Z})^{-1}$. Покажем, что матрица B, задаваемая формулами (13) и (12), является правой обратной для матрицы A.

Ввиду следствия 10 последние два столбца матрицы AB будут такими же, как и у матрицы E. Кроме того, из следствия 10 вытекает, что второй столбец матрицы

$$\begin{pmatrix} b_2+p^n\mathbf{Z} & b_1+p^n\mathbf{Z} & b_3+p^k\mathbf{Z} \\ a_2+p^n\mathbf{Z} & a_1+p^n\mathbf{Z} & a_3+p^k\mathbf{Z} \\ c_2+p^k\mathbf{Z} & c_1+p^k\mathbf{Z} & c_3+p^k\mathbf{Z} \end{pmatrix}\begin{pmatrix} * & -b_1Q+p^{n-k}b_3c_1F+p^n\mathbf{Z} & * \\ * & b_2Q-p^{n-k}b_3c_2F+p^n\mathbf{Z} & * \\ * & F(b_1c_2-b_2c_1)+p^k\mathbf{Z} & * \end{pmatrix}$$

совпадает со вторым столбцом матрицы E. Так как при $m=n$ множитель s в формуле (9) равен 1, отсюда можно сделать вывод, что первый столбец матрицы AB совпадает с первым столбцом матрицы E. Таким образом, $AB=E$.

Наконец, импликация 4) $\Rightarrow$ 5) устанавливается так же, как в теореме 4. ■

Теорема 12. Пусть $m>n>k>0$. Для матрицы $A\in R_3$ вида (6) равносильны следующие условия:

1) Числа a_1, b_2 и c_3 не делятся на p.

2) Элемент $|A|$ обратим в кольце $\mathbf{Z}/p^k\mathbf{Z}$.

3) Матрица A обратима слева в кольце R_3.

4) Матрица A обратима справа в кольце R_3.

5) Матрица A обратима в кольце R_3.

Если эти условия выполнены, то матрица A^{-1} имеет вид

$$\begin{pmatrix} W(1+p^{m-n}a_2b_1G)+p^{m-k}FGU+p^m\mathbf{Z} & * & * \\ -b_1Q+p^{n-k}b_3c_1F+p^n\mathbf{Z} & * & * \\ F(b_1c_2-b_2c_1)+p^k\mathbf{Z} & * & * \end{pmatrix}, \tag{14}$$

где второй и третий столбцы берутся из матрицы (11), а целые числа F, G, Q, W, U задаются условиями

$$F+p^k\mathbf{Z}=|A|^{-1}\in\mathbf{Z}/p^k\mathbf{Z},\ G+p^n\mathbf{Z}=(a_1b_2-p^{m-n}a_2b_1+p^n\mathbf{Z})^{-1}\in\mathbf{Z}/p^n\mathbf{Z},$$

$$M=a_1b_3c_2+p^{m-n}(a_3b_2c_1-a_3b_1c_2-a_2b_3c_1),\ Q=G(1+p^{n-k}FM),$$

$$W+p^m\mathbf{Z}=(a_1+p^m\mathbf{Z})^{-1}\in\mathbf{Z}/p^m\mathbf{Z},\ U=(a_2b_3-a_3b_2)(b_1c_2-b_2c_1).$$

Доказательство. Импликации 5) $\Rightarrow$ 3) $\Rightarrow$ 2) верны по тем же причинам, что и в теореме 11. Так как $m > n > k$, мы можем записать следующие эквивалентности:

$$|A| \text{ – обратимый элемент в } \mathbf{Z}/p^k\mathbf{Z} \Leftrightarrow \text{НОД}(a_1b_2c_3, p) = 1 \Leftrightarrow$$
$$\Leftrightarrow \text{НОД}(a_1, p) = \text{НОД}(b_2, p) = \text{НОД}(c_3, p) = 1.$$

Таким образом, условия 1) и 2) равносильны.

2) $\Rightarrow$ 4). Пусть $|A|$ – обратимый элемент в $\mathbf{Z}/p^k\mathbf{Z}$. Так как справедлива импликация 2) $\Rightarrow$ 1), то числа a_1 и b_2 не делятся на p, т.е. существуют смежные классы $G+p^n\mathbf{Z} = (a_1b_2-p^{m-n}a_2b_1+p^n\mathbf{Z})^{-1}$ и $W+p^m\mathbf{Z} = (a_1+p^m\mathbf{Z})^{-1}$. Покажем, что матрица B, задаваемая формулами (14) и (11), является правой обратной для матрицы A.

Заметим, что справедливы равенства

$$p^{m-n}U = p^{m-n}(a_2b_1b_3c_2 - a_2b_2b_3c_1 - a_3b_1b_2c_2 + a_3b_2b_2c_1) =$$
$$= b_2(a_1b_3c_2 + p^{m-n}a_3b_2c_1 - p^{m-n}a_3b_1c_2 - p^{m-n}a_2b_3c_1) +$$
$$+ p^{m-n}a_2b_1b_3c_2 - a_1b_2b_3c_2 = b_2M - b_3c_2(a_1b_2 - p^{m-n}a_2b_1),$$

а значит, $p^{m-k}U = p^{n-k}b_2M - p^{n-k}b_3c_2(a_1b_2-p^{m-n}a_2b_1)$. Далее, так как $m > n > k$, то

$$G(a_1b_2-p^{m-n}a_2b_1)+p^k\mathbf{Z} = 1+p^k\mathbf{Z},\ a_1W+p^k\mathbf{Z} = 1+p^k\mathbf{Z},$$
$$p^{m-k}G(a_1b_2-p^{m-n}a_2b_1)+p^m\mathbf{Z} = p^{m-k}+p^m\mathbf{Z},\ a_1W+p^n\mathbf{Z} = 1+p^n\mathbf{Z}.$$

В силу леммы 9 нам будет достаточно убедиться, что элементы x_{i1} первого столбца матрицы $X = AB$ совпадают с соответствующими элементами матрицы E. Напомним, что $|A| = a_1b_2c_3 - p^{m-n}a_2b_1c_3 - p^{n-k}M + p^k\mathbf{Z}$. Имеем

$$x_{11} = a_1[W(1+p^{m-n}a_2b_1G)+p^{m-k}FGU]+p^{m-n}a_2(-b_1Q+p^{n-k}b_3c_1F)+$$
$$+p^{m-k}a_3F(b_1c_2-b_2c_1)+p^m\mathbf{Z} = 1+p^{m-n}a_2b_1G+a_1FG\cdot p^{m-k}U-$$
$$-p^{m-n}a_2b_1G(1+p^{n-k}FM)+p^{m-k}a_2b_3c_1F+p^{m-k}F(a_3b_1c_2-a_3b_2c_1)+p^m\mathbf{Z} =$$
$$= 1-p^{m-n}a_2b_1G\cdot p^{n-k}FM+a_1FG[p^{n-k}b_2M-p^{n-k}b_3c_2(a_1b_2-p^{m-n}a_2b_1)]+$$
$$+p^{m-k}F(a_2b_3c_1+a_3b_1c_2-a_3b_2c_1)+p^m\mathbf{Z} =$$
$$= 1-p^{m-k}a_2b_1FGM+p^{n-k}a_1b_2FGM-p^{n-k}a_1b_3c_2FG(a_1b_2-p^{m-n}a_2b_1)+$$
$$+p^{m-k}G(a_1b_2-p^{m-n}a_2b_1)F(a_2b_3c_1+a_3b_1c_2-a_3b_2c_1)+p^m\mathbf{Z} =$$
$$= 1+p^{n-k}FGM(a_1b_2-p^{m-n}a_2b_1)-p^{n-k}a_1b_3c_2FG(a_1b_2-p^{m-n}a_2b_1)+$$
$$+p^{n-k}FG(a_1b_2-p^{m-n}a_2b_1)(p^{m-n}a_2b_3c_1+p^{m-n}a_3b_1c_2-p^{m-n}a_3b_2c_1)+p^m\mathbf{Z} =$$
$$= 1+p^{n-k}FG(a_1b_2-p^{m-n}a_2b_1)(M-a_1b_3c_2)+$$
$$+p^{n-k}FG(a_1b_2-p^{m-n}a_2b_1)(a_1b_3c_2-M)+p^m\mathbf{Z} = 1+p^m\mathbf{Z};$$

$$x_{21} = b_1[W(1+p^{m-n}a_2b_1G)+p^{m-k}FGU]+b_2(-b_1Q+p^{n-k}b_3c_1F)+$$
$$+p^{n-k}b_3F(b_1c_2-b_2c_1)+p^n\mathbf{Z} = b_1W(1+p^{m-n}a_2b_1G)+b_1FG\cdot p^{m-k}U-$$
$$-b_1b_2G(1+p^{n-k}FM)+p^{n-k}b_2b_3c_1F+p^{n-k}F(b_1b_3c_2-b_2b_3c_1)+p^n\mathbf{Z} =$$
$$= b_1W[G(a_1b_2-p^{m-n}a_2b_1)+p^{m-n}a_2b_1G]+$$
$$+b_1FG[p^{n-k}b_2M-p^{n-k}b_3c_2(a_1b_2-p^{m-n}a_2b_1)]-b_1b_2G-p^{n-k}b_1b_2FGM+$$
$$+p^{n-k}b_1b_3c_2F+p^n\mathbf{Z} = b_1W\cdot a_1b_2G-b_1b_2G+p^{n-k}b_1b_2FGM-$$
$$-p^{n-k}b_1b_3c_2FG(a_1b_2-p^{m-n}a_2b_1)-p^{n-k}b_1b_2FGM+p^{n-k}b_1b_3c_2F+p^n\mathbf{Z} =$$
$$= b_1b_2G-b_1b_2G-p^{n-k}b_1b_3c_2F+p^{n-k}b_1b_3c_2F+p^n\mathbf{Z} = 0+p^n\mathbf{Z};$$

$$x_{31} = c_1[W(1+p^{m-n}a_2b_1G)+p^{m-k}FGU]+c_2(-b_1Q+p^{n-k}b_3c_1F)+$$
$$+c_3F(b_1c_2-b_2c_1)+p^k\mathbf{Z} = c_1W(1+p^{m-n}a_2b_1G)+c_1FG\cdot p^{m-k}U-$$
$$-b_1c_2G(1+p^{n-k}FM)+p^{n-k}b_3c_1c_2F+c_3F(b_1c_2-b_2c_1)+p^k\mathbf{Z} =$$
$$= c_1W[G(a_1b_2-p^{m-n}a_2b_1)+p^{m-n}a_2b_1G]+$$
$$+c_1FG[p^{n-k}b_2M-p^{n-k}b_3c_2(a_1b_2-p^{m-n}a_2b_1)]-b_1c_2G-p^{n-k}b_1c_2FGM+$$
$$+p^{n-k}b_3c_1c_2F+c_3F(b_1c_2-b_2c_1)+p^k\mathbf{Z} = c_1W\cdot a_1b_2G+p^{n-k}b_2c_1FGM-$$
$$-p^{n-k}b_3c_1c_2FG(a_1b_2-p^{m-n}a_2b_1)-b_1c_2G-p^{n-k}b_1c_2FGM+$$
$$+p^{n-k}b_3c_1c_2F+c_3FG(a_1b_2-p^{m-n}a_2b_1)(b_1c_2-b_2c_1)+p^k\mathbf{Z} =$$
$$= b_2c_1G+p^{n-k}FGM(b_2c_1-b_1c_2)-p^{n-k}b_3c_1c_2F-b_1c_2G+$$
$$+p^{n-k}b_3c_1c_2F-FG(a_1b_2c_3-p^{m-n}a_2b_1c_3)(b_2c_1-b_1c_2)+p^k\mathbf{Z} =$$
$$= (b_2c_1-b_1c_2)G[1+p^{n-k}FM-F(a_1b_2c_3-p^{m-n}a_2b_1c_3)]+p^k\mathbf{Z} =$$
$$= (b_2c_1-b_1c_2)G[1-F(a_1b_2c_3-p^{m-n}a_2b_1c_3-p^{n-k}M)]+p^k\mathbf{Z} =$$
$$= (b_2c_1-b_1c_2)G[(1+p^k\mathbf{Z})-(F+p^k\mathbf{Z})\cdot|A|] = 0+p^k\mathbf{Z}.$$

Таким образом, $AB = E$.

Импликация 4) $\Rightarrow$ 5) устанавливается так же, как в теореме 4. ■

Если $m = n = k$, то вопрос об обратимости матриц в R_3 решается в соответствии с теоремой 3. Таким образом, остаётся рассмотреть случай $m > n = k$.

Теорема 13. Пусть $m > n = k > 0$. Для матрицы $A \in R_3$ вида (6) равносильны следующие условия:

1) Числа a_1 и $b_2c_3-b_3c_2$ не делятся на p.

2) Элемент $|A|$ обратим в кольце $\mathbf{Z}/p^k\mathbf{Z}$.

3) Матрица A обратима слева в кольце R_3.

4) Матрица A обратима справа в кольце R_3.

5) Матрица A обратима в кольце R_3.

Если эти условия выполнены, то матрица A^{-1} имеет вид

$$\begin{pmatrix} W(1+p^{m-n}FL)+p^m\mathbf{Z} & F(a_3c_2-a_2c_3)+p^k\mathbf{Z} & * \\ F(b_3c_1-b_1c_3)+p^k\mathbf{Z} & F(a_1c_3-p^{m-n}a_3c_1)+p^k\mathbf{Z} & * \\ F(b_1c_2-b_2c_1)+p^k\mathbf{Z} & F(p^{m-n}a_2c_1-a_1c_2)+p^k\mathbf{Z} & * \end{pmatrix}, \tag{15}$$

где третий столбец берётся из матрицы (10), $L = a_2b_1c_3-a_3b_1c_2-a_2b_3c_1+a_3b_2c_1 \in \mathbf{Z}$, $F+p^k\mathbf{Z} = |A|^{-1} \in \mathbf{Z}/p^k\mathbf{Z}$ и $W+p^m\mathbf{Z} = (a_1+p^m\mathbf{Z})^{-1} \in \mathbf{Z}/p^m\mathbf{Z}$.

Доказательство. Импликации 5) $\Rightarrow$ 3) $\Rightarrow$ 2) справедливы по тем же причинам, что и в теореме 11. Далее, так как $n = k$, то $|A| = \delta+p^k\mathbf{Z}$, где

$$\delta = a_1b_2c_3-a_1b_3c_2-p^{m-n}(a_2b_1c_3-a_3b_1c_2-a_2b_3c_1+a_3b_2c_1) =$$
$$= a_1b_2c_3-a_1b_3c_2-p^{m-n}L.$$

Поскольку $m > n$, мы можем записать следующие эквивалентности:

$$|A| \text{ – обратимый элемент в } \mathbf{Z}/p^k\mathbf{Z} \Leftrightarrow \text{НОД}(a_1b_2c_3-a_1b_3c_2, p) = 1 \Leftrightarrow$$
$$\Leftrightarrow \text{НОД}(a_1, p) = \text{НОД}(b_2c_3-b_3c_2, p) = 1.$$

Таким образом, условия 1) и 2) равносильны.

2) $\Rightarrow$ 4). Пусть $|A|$ – обратимый элемент в $\mathbf{Z}/p^k\mathbf{Z}$. Так как справедлива импликация 2) $\Rightarrow$ 1), то a_1 не делится на p, т.е. существует элемент $W+p^m\mathbf{Z} = (a_1+p^m\mathbf{Z})^{-1}$. Поскольку $m > k$, то $a_1W+p^k\mathbf{Z} = 1+p^k\mathbf{Z}$. Убедимся, что матрица B, определяемая формулами (15) и (10), является правой обратной для матрицы A.

По лемме 8 третий столбец матрицы AB будет таким же, как и у матрицы E. Кроме того, из леммы 8 вытекает, что третий столбец матрицы

$$\begin{pmatrix} a_1+p^m\mathbf{Z} & a_3+p^k\mathbf{Z} & a_2+p^k\mathbf{Z} \\ c_1+p^k\mathbf{Z} & c_3+p^k\mathbf{Z} & c_2+p^k\mathbf{Z} \\ b_1+p^k\mathbf{Z} & b_3+p^k\mathbf{Z} & b_2+p^k\mathbf{Z} \end{pmatrix}\begin{pmatrix} * & * & F(a_3c_2-a_2c_3)+p^k\mathbf{Z} \\ * & * & F(p^{m-n}a_2c_1-a_1c_2)+p^k\mathbf{Z} \\ * & * & F(a_1c_3-p^{m-n}a_3c_1)+p^k\mathbf{Z} \end{pmatrix}$$

совпадает с третьим столбцом матрицы E. Так как при $n=k$ множитель t в формуле (9) равен 1, отсюда можно сделать вывод, что второй столбец матрицы AB совпадает со вторым столбцом матрицы E. Остаётся рассмотреть элементы x_{i1} первого столбца матрицы $X=AB$:

$$\begin{gathered} x_{11}=a_1W(1+p^{m-n}FL)+p^{m-n}a_2F(b_3c_1-b_1c_3)+ \\ +p^{m-n}a_3F(b_1c_2-b_2c_1)+p^m\mathbf{Z}=1+p^{m-n}FL+ \\ +p^{m-n}F(a_2b_3c_1-a_2b_1c_3+a_3b_1c_2-a_3b_2c_1)+p^m\mathbf{Z}= \\ =1+p^{m-n}FL-p^{m-n}FL+p^m\mathbf{Z}=1+p^m\mathbf{Z}; \end{gathered}$$

$$\begin{gathered} x_{21}=b_1W(1+p^{m-n}FL)+b_2F(b_3c_1-b_1c_3)+b_3F(b_1c_2-b_2c_1)+p^k\mathbf{Z}= \\ =b_1W(1+p^{m-n}FL)+F(b_1b_3c_2-b_1b_2c_3)+p^k\mathbf{Z}= \\ =b_1W(1+F\cdot p^{m-n}L)+b_1F(b_3c_2-b_2c_3)+p^k\mathbf{Z}= \\ =b_1W[1+F(a_1b_2c_3-a_1b_3c_2-\delta)]+b_1a_1WF(b_3c_2-b_2c_3)+p^k\mathbf{Z}= \\ =b_1W[1+F(a_1b_2c_3-a_1b_3c_2)-F\delta+F(a_1b_3c_2-a_1b_2c_3)]+p^k\mathbf{Z}= \\ =b_1W(1-F\delta)+p^k\mathbf{Z}=b_1W(1-1)+p^k\mathbf{Z}=0+p^k\mathbf{Z}; \end{gathered}$$

$$\begin{gathered} x_{31}=c_1W(1+p^{m-n}FL)+c_2F(b_3c_1-b_1c_3)+c_3F(b_1c_2-b_2c_1)+p^k\mathbf{Z}= \\ =c_1W(1+p^{m-n}FL)+F(b_3c_1c_2-b_2c_1c_3)+p^k\mathbf{Z}= \\ =c_1W(1+F\cdot p^{m-n}L)+c_1F(b_3c_2-b_2c_3)+p^k\mathbf{Z}= \\ =c_1W[1+F(a_1b_2c_3-a_1b_3c_2-\delta)]+c_1a_1WF(b_3c_2-b_2c_3)+p^k\mathbf{Z}= \\ =c_1W[1+F(a_1b_2c_3-a_1b_3c_2)-F\delta+F(a_1b_3c_2-a_1b_2c_3)]+p^k\mathbf{Z}= \\ =c_1W(1-F\delta)+p^k\mathbf{Z}=c_1W(1-1)+p^k\mathbf{Z}=0+p^k\mathbf{Z}. \end{gathered}$$

Тем самым мы показали, что $AB=E$.

Импликация 4) $\Rightarrow$ 5) устанавливается так же, как в теореме 4. ■

В частности, из теорем 11, 12 и 13 вытекает, что обратимость матрицы $A\in R_3$ эквивалентна обратимости элемента $|A|\in\mathbf{Z}/p^k\mathbf{Z}$ в каждом из возможных случаев. Так как обратная матрица единственна (если она существует), то формулы, найденные для A^{-1} в каждой из этих трёх теорем, будут приводить к одной и той же матрице вне зависимости от выбора конкретных чисел $a_j, b_j, c_j\in\mathbf{Z}$, удовлетворяющих равенству (6).

ЛИТЕРАТУРА

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. *Крылов П.А.*, *Туганбаев А.А.* Кольца формальных матриц и модули над ними. М.: МЦНМО, 2017.
3. *Green E.L.* On the representation theory of rings in matrix form // Pacific J. Math. 1982. V. 100. No. 1. P. 123–138. DOI: 10.2140/pjm.1982.100.123.
4. *Haghany A.*, *Varadarajan K.* Study of modules over formal triangular matrix rings // J. Pure Appl. Algebra. 2000. V. 147. No. 1. P. 41–58. DOI: 10.1016/S0022-4049(98)00129-7.

5. *Крылов П.А.*, *Туганбаев А.А.* Формальные матрицы и их определители // Фундам. и прикл. математика. 2014. Т. 19. № 1. С. 65–119.
6. *Крылов П.А.* Определители обобщённых матриц порядка 2 // Фундам. и прикл. математика. 2015. Т. 20. № 5. С. 95–112.
7. *Глухов М.М.*, *Елизаров В.П.*, *Нечаев А.А.* Алгебра. Т. 1. М.: Гелиос АРВ, 2003.

Статья поступила 09.08.2021

Stepanova A.Y., Timoshenko E.A. (2021) 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

Keywords: primary group, endomorphism ring, generalized matrix ring, inverse matrix.

Let p be a prime. Any finite Abelian p-group H of rank 2 can be identified with a group of the form $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z})$ with $m \ge n > 0$. The endomorphisms of this group H are in a one-to-one correspondence with elements of the following set of matrices:

$$R_2 = \begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} \end{pmatrix}.$$

If we define $\begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix}\begin{pmatrix} a'+p^m\mathbf{Z} & b'+p^n\mathbf{Z} \\ c'+p^n\mathbf{Z} & d'+p^n\mathbf{Z} \end{pmatrix}$ to be

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

then we arrive at the following theorem:

Theorem 1. The set R_2 with entrywise addition and multiplication defined above forms a ring which is isomorphic to the endomorphism ring End H of H. The identity element of R_2 is

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

For any $A = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \in R_2$, we define $|A| = ad - p^{m-n}bc + p^n\mathbf{Z} \in \mathbf{Z}/p^n\mathbf{Z}$.

Proposition 2. For any $A, A' \in R_2$, we have $|AA'| = |A| \cdot |A'|$.

If $m = n$, then R_2 is the usual matrix ring over $\mathbf{Z}/p^n\mathbf{Z}$ and the invertibility criterion for $A \in R_2$ is well-known.

Theorem 4. Let $m > n > 0$. For any matrix $A = \begin{pmatrix} a+p^m\mathbf{Z} & b+p^n\mathbf{Z} \\ c+p^n\mathbf{Z} & d+p^n\mathbf{Z} \end{pmatrix} \in R_2$, the following are equivalent:

1) The prime p does not divide a and d.
2) The element $|A|$ is invertible in $\mathbf{Z}/p^n\mathbf{Z}$.
3) The matrix A is left invertible in R_2.
4) The matrix A is right invertible in R_2.
5) The matrix A is invertible in R_2.

If these conditions are satisfied, then

$$A^{-1} = \begin{pmatrix} W(1+p^{m-n}bcF)+p^m\mathbf{Z} & -bF+p^n\mathbf{Z} \\ -cF+p^n\mathbf{Z} & aF+p^n\mathbf{Z} \end{pmatrix},$$

where $F + p^n\mathbf{Z} = |A|^{-1} \in \mathbf{Z}/p^n\mathbf{Z}$ and $W + p^m\mathbf{Z} = (a + p^m\mathbf{Z})^{-1} \in \mathbf{Z}/p^m\mathbf{Z}$.

Any finite Abelian p-group H of rank 3 can be identified with a suitable group of the form $(\mathbf{Z}/p^m\mathbf{Z}) \oplus (\mathbf{Z}/p^n\mathbf{Z}) \oplus (\mathbf{Z}/p^k\mathbf{Z})$ with $m \ge n \ge k > 0$. The endomorphisms of this group H are in one-to-one correspondence with the elements of the following set of matrices:

$$R_3 = \begin{pmatrix} \mathbf{Z}/p^m\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} \\ \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^n\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} \\ \mathbf{Z}/p^k\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} & \mathbf{Z}/p^k\mathbf{Z} \end{pmatrix}.$$

As in the case of R_2, we endow R_3 with a multiplication such that R_3 becomes a ring which is isomorphic to End H.

For any matrix $A = \begin{pmatrix} a_1 + p^m\mathbf{Z} & a_2 + p^n\mathbf{Z} & a_3 + p^k\mathbf{Z} \\ b_1 + p^n\mathbf{Z} & b_2 + p^n\mathbf{Z} & b_3 + p^k\mathbf{Z} \\ c_1 + p^k\mathbf{Z} & c_2 + p^k\mathbf{Z} & c_3 + p^k\mathbf{Z} \end{pmatrix} \in R_3$, we denote by $|A|$ the element

$$a_1b_2c_3 - p^{n-k}a_1b_3c_2 - p^{m-n}a_2b_1c_3 + p^{m-k}(a_3b_1c_2 + a_2b_3c_1 - a_3b_2c_1) + p^k\mathbf{Z}.$$

Proposition 6. For any $A, A' \in R_3$, we have $|AA'| = |A| \cdot |A'|$.

The case when $m = n = k$ is trivial. For the cases $m = n > k$, $m > n > k$ and $m > n = k$, we give invertibility criteria for $A \in R_3$ and formulas for inverse matrices. In each of these cases the following are equivalent:

- The element $|A|$ is invertible in $\mathbf{Z}/p^k\mathbf{Z}$.
- The matrix A is left invertible in R_3.
- The matrix A is right invertible in R_3.
- The matrix A is invertible in R_3.

AMS Mathematical Subject Classification: 16S50

Financial support. This work was supported by the Ministry of Science and Higher Education of Russia (agreement No. 075-02-2021-1392).

Aleksandra Y. STEPANOVA (Tomsk State University, Tomsk, Russian Federation). E-mail: stepanova.alexa@mail.ru

Egor A. TIMOSHENKO (Doctor of Physics and Mathematics, Tomsk State University, Tomsk, Russian Federation). E-mail: tea471@mail.tsu.ru

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. Krylov P., Tuganbaev A. (2017) *Formal Matrices* (Algebra and Applications, Vol. 23). Springer. DOI: 10.1007/978-3-319-53907-2.
3. Green E.L. (1982) On the representation theory of rings in matrix form. *Pacific Journal of Mathematics*. 100(1). pp. 123–138. DOI: 10.2140/pjm.1982.100.123.
4. Haghany A., Varadarajan K. (2000) Study of modules over formal triangular matrix rings. *Journal of Pure and Applied Algebra*. 147(1). pp. 41–58. DOI: 10.1016/S0022-4049(98)00129-7.
5. 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.
6. 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.
7. Glukhov M.M., Elizarov V.P., Nechaev A.A. (2003) *Algebra* [Algebra]. Vol. 1. Moscow: Gelios ARV.

Received: August 9, 2021