УДК 512.541+512.542

***ПОПОВ Иван Николаевич**, кандидат физико-математических наук, доцент кафедры математики института математики, информационных и космических технологий Северного (Арктического) федерального университета имени М.В. Ломоносова. Автор 38 научных публикаций*

КОЛИЧЕСТВО РАЗЛОЖЕНИЙ МАТРИЦ В ПОДГРУППЕ ГРУППЫ RC

В статье изложены результаты исследований группы RC_n. Элементами группы *RC* являются квадратные матрицы над полем Z_2 размерности *n*, операция в группе – сложение матриц. Любая матрица из конечной аддитивной группы *RC* имеет порядок 2 и представляется в виде суммы так называемых матриц-строк и матриц-столбцов, множество которых является носителем элемента группы. Каждая матрица из группы *RC* имеет ровно два различных носителя.

Любую подгруппу группы *RC* можно рассматривать как линейную оболочку матриц, которые называются образующими оболочки. Оболочка может иметь несколько наборов образующих. Среди всех образующих линейной оболочки выделяют так называемые фундаментальные системы, через каждую из которых любой элемент оболочки выражается единственным образом.

В работе рассматривается вопрос о количестве разложений матриц в подгруппе группы *RC*, заданной в виде линейной оболочки с определенным числом образующих. Устанавливается связь между количеством разложений произвольной матрицы с количеством разложений нулевой матрицы через образующие линейной оболочки. Формулируется и доказывается теорема, в которой утверждается, что количество разложений матрицы в подгруппе группы *RC* равно количеству разложений нулевой матрицы в этой подгруппе. В связи с этим предлагается формула для определения количества всех разложений нулевой матрицы в произвольной подгруппе группы *RC*. В статье затрагивается вопрос о фундаментальной системе образующих подгруппы группы *RC*. Показывается ее роль в определении порядка линейной оболочки как подгруппы группы *RC*, так и самой группы *RC*.

***Ключевые слова:** порядок группы, линейная оболочка, фундаментальная система образующих.*

Группа *RC*. Пусть $N = \{1; 2; \dots ; n\}$ – множество натуральных чисел от 1 до *n*, где *n* – натуральное число, отличное от 1.

Пусть $Z_2 = \{0; 1\}$. Определим сложение на этом множестве следующим образом: $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$. Очевидно, что Z_2 является группой относительно введенного сложения.

Пусть $M_n(Z_2)$ – множество всех квадратных матриц порядка *n* с элементами из множества Z_2. Нулевую матрицу обозначим Θ. С обычным сложением матриц множество $M_n(Z_2)$ есть абе-

лева группа. Очевидно, что любая матрица A группы $M_n(Z_2)$ имеет порядка 2, т. е. $A = A = \Theta$. Естественно считать, что $0 \times A = \Theta$ и $1 \times A = A$ для любой матрицы $A \in M_n(Z_2)$.

Ясно, что $|M_n(Z_2)| = 2^{n^2}$. По теореме Лагранжа для конечных групп получаем, что порядок любой подгруппы группы $M_n(Z_2)$ есть степень числа 2.

Рассмотрим матрицы следующего вида: E_i – квадратная матрица порядка n, в которой все элементы i-й строки равны 1, а остальные – 0; E^j – квадратная матрица порядка n, в которой все элементы j-го столбца равны 1, а остальные – 0. Матрицу E_i будем называть матрицей-строкой с номером i, а матрицу E_j – матрицей-столбцом с номером j. Здесь $i, j \in N$.

Пример. Для случаев $n = 2$ и $n = 3$ соответственно получаем:

$$E_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},\ E_2 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix},\ E^1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix},$$

$$E^2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(Z_2);$$

$$E_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

$$E^1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, E^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, E^3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(Z_2).$$

Для произвольного случая количество матриц-строк, также как и матриц-столбцов, равно n. ■

Введем в рассмотрение подгруппу RC группы $M_n(Z_2)$, порожденную матрицами-строками $E_1, E_2, \ldots, E_n$ и матрицами-столбцами $E^1, E^2, \ldots, E^n$, т. е. каждая матрица группы RC есть сумма вида:

$$\sum_{i=1}^{n} (x_i E_i + y_i E^i) = x_1 E_1 + x_2 E_2 + \ldots + x_n E_n + y_1 E^1 + y_2 E^2 + \ldots + y_n E^n,$$

где $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in Z_2$.

При необходимости у символа RC_n нижним индексом будем указывать размерность матриц n, входящих в нее. Заметим, что порядок группы RC_n есть степень числа 2.

Пусть $A \in RC$. Тогда матрицу A можно записать в виде:

$$A = E_{i_1} + E_{i_2} + \ldots + E_{i_k} + E^{j_1} + E^{j_2} + \ldots + E^{j_\ell},$$

где $0 \le k \le n$, $0 \le \ell \le n$ и $i_1, i_2, \ldots, i_k$, также как и $i_1, i_2, \ldots, i_\ell$, – попарно различные числа из множества N. Будем говорить, что представлено разложение матрицы A через матрицы $E_{i_1}, \ldots, E_{i_k}$ и $E^{j_1}, \ldots, E^{j_\ell}$, или матрица A выражается через эти матрицы. При этом если $k = 0$, то будем считать, что в разложение матрицы A ни одна из матриц-строк не входит, если же $\ell = 0$, то в разложение не входит ни одна матрица-столбец.

Отметим, что в разложение матрицы из группы RC каждая матрица-строка и матрица-столбец из множества $\{E_1; \ldots; E_n; E^1 \ldots; E^n\}$ входит не более одного раза.

Пусть $A \in RC$ и

$$A = E_{i_1} + E_{i_2} + \ldots + E_{i_k} + E^{j_1} + E^{j_2} + \ldots + E^{j_\ell},$$

где $i_1, i_2, \ldots, i_k$, также как и $i_1, i_2, \ldots, i_\ell$, – попарно различные числа из множества N, где $0 \le k \le n$ и $0 \le \ell \le n$. Множество

ùùùùùùùù= $E_{i_1}\ E_{i_2}\ \ldots\ E_{i_k}\ E^{j_1}\ E^{j_2}\ \ldots\ E^{j_\ell}$

назовем носителем матрицы A. В носителе матрицы из группы RC все матрицы попарно различны. Отметим, что не предполагается, что носитель матрицы определен для него однозначно. Будем считать, что носитель нулевой матрицы из группы RC, матрица Θ, в частности, может быть и пустым, и равенство $\Theta = \Theta$ будем рассматривать как разложение матрицы Θ в группе RC. Отметим, что нулевой элемент не входит в носитель никакой матрицы из группы RC.

Пример. Из справедливости равенства $E_1 + E_1 = \Theta$ не вправе написать, что $\mathrm{supp}(\Theta) = \{E_1\}$. ■

В частности, носитель каждой матрицы из множества $\{E_1; \ldots; E_n; E^1; \ldots E^n\}$ равен самому элементу.

Теорема (характеристическое свойство матриц из группы RC_n). Матрица группы $M_n(Z_2)$

принадлежит группе RC_n тогда и только тогда, когда суммы первой строки (первого столбца) и любой другой строки (любого другого столбца) как векторов есть вектор, все элементы которого одновременно равны 0 или 1.

Пример. Рассмотрим две матрицы из группы $M_4(Z_2)$:

$$A=\begin{pmatrix}1&1&0&0\\0&0&1&1\\1&1&0&0\\1&1&0&0\end{pmatrix} \quad \text{и} \quad B=\begin{pmatrix}1&1&0&0\\0&1&1&1\\1&1&0&0\\1&1&0&0\end{pmatrix}.$$

Так как суммы первой строки и любой другой строки матрицы A есть вектор (1; 1; 1; 1) или (0; 0; 0; 0), все элементы которого равны 1 или 0, то матрица A удовлетворяет характеристическому свойству матриц из группы RC_4, значит, $A \in RC_4$.

Для матрицы B справедливо: сумма первой и второй строк есть вектор (1; 0; 1; 1), который не совпадает ни с вектором (0; 0; 0; 0), ни с вектором (1; 1; 1; 1). Значит, $B \notin RC_4$. ■

Общие вопросы теории групп изложены в работе [1]. Более подробно о группе RC_n можно ознакомиться в монографии [2].

Линейные оболочки матриц из группы *RC*. Порядок группы H, то есть количество ее элементов, будем обозначать символом $|H|$.

Пусть $A_1, A_2, \ldots, A_m$ – ненулевые матрицы из группы RC_n. Множество вида

$$F=\langle A_1; A_2; \ldots; A_m\rangle =$$

$$=\{\varepsilon_1 A_1+\varepsilon_2 A_2+\ldots+\varepsilon_m A_m \mid \varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m \in Z_2\}$$

назовем линейной оболочкой матриц $A_1, A_2, \ldots, A_m$. Сами матрицы $A_1, A_2, \ldots, A_m$ назовем образующими линейной оболочки F. Если матрица A из группы RC_n принадлежит линейной оболочке $\langle A_1, A_2, \ldots, A_m\rangle$, то будем говорить, что матрица A раскладывается (выражается) через матрицы $A_1, A_2, \ldots, A_m$. Равенство

$$A = C_1 + \ldots + C_k,$$

где $C_1, \ldots, C_k$ – попарно различные матрицы из множества $\{A_1, A_2, \ldots, A_m\}$, где $1 \le k \le m$, назовем разложением матрицы A. Множество $\{C_1; \ldots; C_k\}$ назовем носителем матрицы A, обозначим его символом supp(A). Договоримся, что для нулевой матрицы Θ равенство $\Theta = \Theta$ является ее разложением, носитель которого равен пустому множеству. В этом случае справедливо: $\varnothing^+ = \Theta$.

Очевидно, что линейная оболочка $\langle A_1; A_2; \ldots; A_m\rangle$ является подгруппой группы RC_n, которой, в частности, принадлежат сами матрицы $A_1; A_2; \ldots; A_m$ и нулевая матрица Θ. Поэтому $|\langle A_1; A_2; \ldots; A_m\rangle| \ge m+1$.

Пусть матрица $A \in \langle A_1; A_2; \ldots; A_m\rangle$ имеет разложения:

$A = C_1 + \ldots + C_k$ и $A = D_1 + \ldots + D_\ell$,

где $C_1, \ldots, C_k$, , также как и $D_1, \ldots, D_\ell$ – попарно различные матрицы из множества $\{A_1; A_2; \ldots; A_m\}$, , где $1 \le k \le m$ и $1 \le \ell \le m$. Разложения матрицы A через матрицы $C_1, \ldots, C_k$ и $D_1, \ldots, D_\ell$ назовем различными, если множества $\{C_1, \ldots, C_k\}$ и $\{D_1; \ldots; D_\ell\}$ не совпадают.

Пример. Пусть A_1, A_2, A_3 – матрицы из группы RC_2, имеющие вид:

$$A_1=\begin{pmatrix}1&1\\0&0\end{pmatrix},\ A_2=\begin{pmatrix}1&1\\1&1\end{pmatrix},\ A_3=\begin{pmatrix}0&0\\1&1\end{pmatrix}.$$

Линейная оболочка этих матриц состоит из четырех матриц:

$$\langle A_1; A_2; A_3\rangle=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix};\begin{pmatrix}1&1\\0&0\end{pmatrix};\begin{pmatrix}1&1\\1&1\end{pmatrix};\begin{pmatrix}0&0\\1&1\end{pmatrix}\right\}.$$

Справедливы равенства:

$$A_1 = A_1 \text{ и } A_1 = A_2 + A_3,$$

т. е. матрица A_1 имеет два различных разложения в линейной оболочке $\langle A_1; A_2; A_3\rangle$. При этом для первого разложения матрицы A_1 носитель имеет вид supp(A_1) = $\{A_1\}$, для второго – supp(A_1) = $\{A_2; A_3\}$. Нулевая матрица Θ также имеет два разложения:

$$\Theta = \Theta \text{ и } \Theta = A_1 + A_2 + A_3.$$

В первом случае supp(Θ) = $\varnothing$, во втором –. supp(Θ) = $\{A_1; A_2; A_3\}$.

Так как в линейной оболочке $\{A_1; A_2; \ldots; A_m\}$ матрицы могут выражаться через матрицы $\{A_1; A_2; \ldots; A_m\}$ не единственным образом, то порядок линейной оболочки $\langle A_1; A_2; \ldots; A_m\rangle$ не превышает числа 2^m. Тогда

$$m+1 \le |\langle A_1; A_2; \ldots; A_m\rangle| \le 2^m.$$

Количество разложений матрицы из линейной оболочки группы *RC*. Пусть $n \geq 2$. Введем обозначение:

$$U = \left\{E_1; E_2; \ldots; E_n; E^1; E^2; \ldots E^n\right\}.$$

Пусть $F_1; F_2; \ldots; F_k$ – попарно различные непустые подмножества множества U. Тогда $1 \leq k \leq n$. Для каждого $i \in \{1; 2; \ldots; k\}$ символом F_i^+ обозначим сумму всех матриц из множества F_i. Тогда $F_i = \text{supp}(F_i^+)$. Пусть $F = \left\langle F_1^+; F_2^+; \ldots; F_k^+ \right\rangle$.

Теорема. Если матрица Θ имеет m различных разложений в группе F, то и каждая матрица этой группы имеет ровно m различных разложений.

Доказательство. Заметим, из того, что нулевая матрица в группе F имеет разложение $\Theta = \Theta$, следует, что m – натуральное число.

Пусть ненулевая матрица B из группы F имеет больше m различных разложений: $B = C_1$, …., $B = C_m$, $B = C_{m+1}$, ...

Пусть $B = C_S$ – одно из разложений матрицы B, где $1 \leq s \leq m$. Так как разложения $B = C_S$ и $B = C_{m+1}$ различны, то $\text{supp}(C_S + C_{m+1}) \neq \varnothing$.

Пусть $B = C_p$ и $B = C_q$ – различные разложения матрицы B из числа выше указанных, причем $p \neq m + 1$ и $q \neq m + 1$. Очевидно, что $\Theta = C_p + C_{m+1}$ и $\Theta = C_q + C_{m+1}$. Так как $\text{supp}(C_p) \neq \text{supp}(C_q)$, то найдется такая матрица A, что $A \in \text{supp}(C_p)$ и $A \notin \text{supp}(C_q)$. Если $A \in \text{supp}(C_{m+1})$, то

$A \notin \text{supp}(C_p + C_{m+1})$ и $A \in \text{supp}(C_q + C_{m+1})$,

если же $A \notin \text{supp}(C_{m+1})$, то

$A \in \text{supp}(C_p + C_{m+1})$ и $A \notin \text{supp}(C_q + C_{m+1})$.

В любом случае разложения $\Theta = C_p + C_{m+1}$ и $\Theta = C_q + C_{m+1}$ являются различными. Тогда $\Theta = \Theta$, $\Theta = C_1 + C_{m+1}$, …, $\Theta = C_m + C_{m+1}$ – попарно различные разложения нулевой матрицы, что противоречит условию. Значит, каждая матрица из группы F имеет не более m разложений.

Пусть теперь $\Theta = \Theta_1^+$, $\Theta = \Theta_2^+, \ldots$, $\Theta = \Theta_m^+$ – различные разложения нулевой матрицы в группе F. Пусть B – ненулевая матрица из группы F.

Тогда $B = B + \Theta = B + \Theta_1^+$, $B = B + \Theta = B + \Theta_2^+$ … , $B = B + \Theta = B + \Theta_m^+$ – разложения матрицы B. Различны ли они попарно? Пусть $B = B + \Theta_i^+$ и $B = B + \Theta_j^+$ – два разложения матрицы B. Так как $\Theta_i \neq \Theta_j$, то найдется матрица A такая, что $A \in \Theta_i$, но $A \notin \Theta_j$. Если $A \in \text{supp}(B)$, то

$A \notin \text{supp}(B + \Theta_i^+)$ и $A \in \text{supp}(B + \Theta_j^+)$,

если же $A \notin \text{supp}(B)$, то

$A \in \text{supp}(B + \Theta_i^+)$ и $A \notin \text{supp}(B + \Theta_j^+)$.

Поэтому разложения $B = B + \Theta_i^+$ и $B = B + \Theta_j^+$ являются различными. Значит, каждая матрица из группы F имеет не менее m различных разложений.

Итак, каждая матрица из группы F имеет ровно m разложений.

Получили, что в группе $F = \left\langle F_1^+; F_2^+; \ldots; F_k^+ \right\rangle$ каждая матрица может быть представлена в виде суммы $\varepsilon_1 F_1^+ + \varepsilon_2 F_2^+ + \ldots + \varepsilon_k F_k^+$ ровно m раз при изменении значений коэффициентов ε_1, ε_2, ... , ε_k, если нулевая матрица раскладывается в группе F m раз через ее образующие.

Из теоремы следует, что если нулевая матрица из группы $F = \left\langle F_1^+; F_2^+; \ldots; F_k^+ \right\rangle$ имеет в ней ровно m разложений, то

$$m \,|\, F \,| = 2^k,$$

значит, порядок группы F равен $\frac{2^k}{m}$, т. е. $|\, F \,| = \frac{2^k}{m}$.

Теорема. Количество разложений нулевой матрицы через образующие $F_1^+, F_2^+, \ldots, F_k^+$ линейной оболочки F равно степени числа 2.

Доказательство. Учитывая, что группа F есть подгруппа группы RC_n, порядок которой равен степени числа 2, то из равенства $|\, F \,| = \frac{2^k}{m}$ получаем, что m – степень числа 2, т. е. $m = 2^\ell$ для некоторого неотрицательного целого числа ℓ.

Из теоремы получаем, что $|\, F \,| = 2^{k-\ell}$.

Пример. Пусть F – подгруппа группы RC_3, состоящая из следующих матриц:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix},\ \begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}1&1&0\\1&1&0\\1&1&0\end{pmatrix},\ \begin{pmatrix}0&0&0\\0&0&0\\1&1&1\end{pmatrix}.$$

Тогда $|F| = 8$. Можно показать, что

$$F=\left\langle\begin{pmatrix}0&1&0\\0&1&0\\1&0&1\end{pmatrix};\begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix};\begin{pmatrix}0&0&0\\0&0&0\\1&1&1\end{pmatrix};\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix};\begin{pmatrix}1&0&0\\1&0&0\\0&1&1\end{pmatrix}\right\rangle.$$

Из матриц, являющихся образующими линейной оболочки F, можно получить нулевую матрицу тремя способами, без повторения и учета следования матриц:

$$\begin{pmatrix}0&1&0\\0&1&0\\1&0&1\end{pmatrix}+\begin{pmatrix}0&0&0\\0&0&0\\1&1&1\end{pmatrix}+\begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix}=\Theta,$$

$$\begin{pmatrix}0&0&0\\0&0&0\\1&1&1\end{pmatrix}+\begin{pmatrix}1&0&0\\1&0&0\\0&1&1\end{pmatrix}+\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}=\Theta,$$

$$\begin{pmatrix}0&1&0\\0&1&0\\1&0&1\end{pmatrix}+\begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix}+\begin{pmatrix}1&0&0\\1&0&0\\0&1&1\end{pmatrix}+\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}=\Theta.$$

И, конечно же, справедливо разложение $\Theta = \Theta$. Всего получаем 4 различных разложений нулевой матрицы, значит, $m = 4$.

Для этой же группы F справедливо также следующее равенство:

$$F=\left\langle\begin{pmatrix}0&1&0\\0&1&0\\1&0&1\end{pmatrix};\begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix};\begin{pmatrix}1&1&0\\1&1&0\\1&1&0\end{pmatrix};\begin{pmatrix}1&0&0\\1&0&0\\0&1&1\end{pmatrix}\right\rangle.$$

При таком задании группы F справедливы только два разложения нулевой матрицы:

$$\begin{pmatrix}0&1&0\\0&1&0\\1&0&1\end{pmatrix}+\begin{pmatrix}1&0&0\\1&0&0\\0&1&1\end{pmatrix}+\begin{pmatrix}1&1&0\\1&1&0\\1&1&0\end{pmatrix}=\Theta \text{ и } \Theta = \Theta.$$

Поэтому $m = 2$.

Из примера видим, что при фиксированном числе n само число m, равное количеству разложений нулевой матрицы через матрицы $F_1^+, F_2^+, \ldots, F_k^+$, являющиеся образующими линейной оболочки F, с учетом разложения $\Theta = \Theta$ зависит от числа k. Поэтому число m будем обозначать символом $m(k)$. Тогда из примера при $n = 3$ получаем, что $m(5) = 4$ и $m(4) = 2$.

Заметим, что символ $m(k)$ определен для чисел k таких, что $1 \le k \le |F|$.

Теорема. Пусть $\Theta_1^+, \Theta_2^+, \ldots, \Theta_{m(k)}^+$ – различные разложения нулевой матрицы через образующие линейной оболочки $F = \langle F_1^+; F_2^+; \ldots; F_k^+ \rangle$, включая и разложение $\Theta = \Theta$. Тогда $\left(\{\Theta_1; \Theta_2; \ldots; \Theta_{m(k)}\}, \Delta\right)$ – абелева группа, где Δ – операция вычисления симметрической разности двух множеств.

Доказательство. Так как учитывается разложение $\Theta = \Theta$, для которого $\text{supp}(\Theta) = \varnothing$, то $\varnothing \in \{\Theta_1; \Theta_2; \ldots; \Theta_{m(k)}\}$.

Для любых i и j из множества $\{1; 2; \ldots; m(k)\}$ справедливы равенства:

$$\left(\Theta_i \Delta \Theta_j\right)^+ = \Theta_i^+ + \Theta_j^+ \text{ и } \Theta_i \Delta \Theta_i = \varnothing.$$

Так как $\Theta_i^+ + \Theta_j^+ = \Theta$, то $\Theta_i \Delta \Theta_j \in \{\Theta_1; \Theta_2; \ldots; \Theta_{m(k)}\}$ Симметрическая разность множеств обладает свойством ассоциативности, т. е. для любых множеств M_1, M_2, M_3 справедливо равенство:

$$(M_1 \Delta M_2) \Delta M_3 = M_1 \Delta (M_2 \Delta M_3).$$

Поэтому $\left(\{\Theta_1; \Theta_2; \ldots; \Theta_{m(k)}\}; \Delta\right)$ – абелева группа. ■

Теорема. Пусть $F = \langle F_1^+; F_2^+; \ldots; F_k^+ \rangle$. Тогда справедлива формула:

$$m(|F|) = m(k) 2^{|F|-k-1}.$$

Доказательство. Пусть $A_1, A_2, \ldots, A_{|F|-1}$ – все ненулевые матрицы из группы F. Тогда

$$F = \langle A_1, A_2, \ldots, A_{|F|-1} \rangle = \{A_1, A_2, \ldots, A_{|F|-1}; \Theta\}.$$

При этом справедливы равенства:

$$m(|F|) \times |F| = 2^{|F|-} \text{ и } m(k) \times |F| = 2^{\cdot}.$$

Тогда $|F| = \dfrac{2^{|F|-1}}{m(|F|)}$ и $|F| = \dfrac{2^k}{m(k)}$, значит, $m(|F|) = m(k) \cdot 2^{|F|-k-1}$. ■

Из формулы $m(|F|) = m(k) \times 2^{|F|-k-}$, зная числа $|F|$ и $m(k)$, можно найти количество всех способов получения нулевой матрицы, как

суммы матриц из группы F, без повторения слагаемых и учета их расположения в сумме, включая разложение $\Theta = \Theta$.

Пример. Для группы

$$F = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle$$

справедливо: $|F| = 8$, $k = 5$ и $m(5) = 4$. Тогда $m(|F|) = m(8) = 4 \times 2^{8-5-1} = 16$.

Так как группа F может быть задана и следующим образом:

$$F = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle,$$

то, учитывая, что $|F| = 8$, $k = 4$ и $m(4) = 2$ получаем:

$$m(|F|) = m(8) = 2 \times 2^{8-4-1} = 16.$$

Итак, в группе F нулевую матрицу можно представить в виде суммы матриц из группы F 16 способами, с учетом разложения $\Theta = \Theta$.

Среди разложений, например, есть следующие:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} = \Theta,$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \Theta.$$

Если сложить все ненулевые матрицы из группы F, то также получаем нулевую матрицу. В этом случае носитель нулевой матрицы содержит 7 матриц. ■

Теорема. Пусть F – линейная оболочка, для которой существуют два набора матриц, ее порождающих, в количествах k и ℓ соответственно. Тогда справедливо: $m(k) = m(\ell)$ тогда и только тогда, когда $k = \ell$.

Доказательство. Пусть $m(k) = m(\ell)$. Так как $m(|F|) = m(k) \cdot 2^{|F|-k-1}$ и $m(|F|) = m(\ell) \cdot 2^{|F|-\ell-1}$, то $2^{|F|-k-1} = 2^{|F|-\ell-1}$, значит, $k = \ell$.

Обратно, если $k = \ell$, то из равенства $m(k) \times 2^{|F|-k-1} = m(\ell) \times 2^{|F|-k-1}$ получаем, что $m(k) = m(\ell)$. ■

Фундаментальная система образующих подгруппы группы *RC*. Матрицу A из множества $\{F_1^+; F_2^+; \ldots; F_k^+\}$ назовем независимой от других матриц этого множества, если матрица A не выражается через матрицы множества $\{F_1^+; F_2^+; \ldots; F_k^+\} \setminus \{A\}$. Если это справедливо для каждой матрицы из множества $\{F_1^+; F_2^+; \ldots; F_k^+\}$, то это множество назовем независимым множеством матриц.

Теорема. Пусть $F = \langle F_1^+; F_2^+; \ldots; F_k^+ \rangle$, где $k \geq 2$. Тогда справедливо: $m(k) = 1$ тогда и только тогда, когда множество $\{F_1^+; F_2^+; \ldots; F_k^+\}$ является независимым множеством матриц.

Доказательство. Пусть $m(k) = 1$. Предположим, что некоторая матрица F_i^+ из множества $\{F_1^+; F_2^+; \ldots; F_k^+\}$ выражается через матрицы множества $\{F_1^+; F_2^+; \ldots; F_k^+\} \setminus \{F_i^+\}$. Тогда $F = \langle F_1^+; \ldots; F_{i-1}^+; F_{i+1}^+; \ldots; F_k^+ \rangle$ и число образующих равно $k - 1$. Из равенств $m(k) = 1$, $m(|F|) = m(k) \times 2^{|F|-k-}$ и $m(|F|) = m(k-1) \cdot 2^{|F|-(k-1)-1}$ следует, что $2m(k-1) = 1$, что не так. Пришли к противоречию. Значит, $\{F_1^+; F_2^+; \ldots; F_k^+\}$ – независимое множество матриц.

Пусть теперь $\{F_1^+; F_2^+; \ldots; F_k^+\}$ – независимое множество матриц. Предположим, что $m(k) \geq 2$. Тогда любая ненулевая матрица из группы F выражается хотя бы двумя способами через матрицы из множества $\{F_1^+; F_2^+; \ldots; F_k^+\}$. Это относится к матрице F_1^+ (одно из разложений этой матрицы имеет вид $F_1^+ = F_1^+$), что противоречит условию. Пришли к противоречию, значит, $m(k) = 1$.

Пусть $F = \langle F_1^+; F_2^+; \ldots; F_k^+ \rangle$ – подгруппа группы RC_n. Если множество $\{F_1^+; F_2^+; \ldots; F_k^+\}$ является независимым множеством матриц (то же самое, что $m(k) = 1$), то будем говорить, что матрицы $F_1^+, F_2^+, \ldots, F_k^+$ образуют фундаментальную систему образующих группы F (ФСО).

Теорема. Любые две фундаментальные системы образующих группы F содержат одно и то же количество матриц.

Доказательство. Пусть в одной ФСО группы F содержится k матриц, а в другой ФСО группы F – ℓ матриц. При этом справедливы равенства: $m(k) = 1$ и $m(\ell) = 1$. Тогда $m(k) = m(\ell)$, откуда $k = \ell$. ■

Итак, фундаментальные системы образующих группы могут отличаться наборами матриц, но не их количеством. Число в некоторой ФСО (значит, в любой) группы F назовем рангом этой группы и обозначим символом rank(F). Заметим, что ранг определяется для любой ненулевой подгруппы F группы RC_n, т. е. $F \neq \{\Theta\}$, т. к. группу F можно считать линейной оболочкой всех своих ненулевых матриц. Тогда справедливо: $1 \le \text{rank}(F) \le |F| - 1$ и $m(\text{rank}(F)) = 1$.

Теорема. Пусть $F = \langle F_1^+; F_2^+; \ldots; F_k^+ \rangle$, где $F_1^+, F_2^+, \ldots, F_k^+$ – ФСО группы F. Тогда любая матрица из группы F единственным образом выражается через матрицы $F_1^+, F_2^+, \ldots, F_k^+$ с точностью до перестановки слагаемых и без учета повторения матриц из этого набора образующих группы F.

Доказательство. Так как $F_1^+, F_2^+, \ldots, F_k^+$ – ФСО группы F, то $m(k) = 1$. Предположим, что некоторая ненулевая матрица A из группы F выражается через матрицы $F_1^+, F_2^+, \ldots, F_k^+$ хотя бы двумя способами. Тогда отсюда следует, что и нулевая матрица будет иметь неединственное разложение, что не так, т. к. $m(k) = 1$. Пришли к противоречию. Следовательно, все матрицы, включая и нулевую матрицу, из группы F единственным образом выражаются через матрицы $F_1^+, F_2^+, \ldots, F_k^+$. ■

Теорема. Пусть $F = \langle F_1^+; F_2^+; \ldots; F_k^+ \rangle$, где $F_1^+, F_2^+, \ldots, F_k^+$ – ФСО группы F. Тогда $|F| = 2^k$ и $m(|F|) = 2^{2^k - k - 1}$.

Пример. Пусть F – подгруппа группы RC_3 такая, что

$$F = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle.$$

Так как только в матрице $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ из трех предложенных матриц элемент в первой строке и первом столбце равен 1, то равенство

$$\varepsilon_1 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \varepsilon_2 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} + \varepsilon_3 \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \Theta$$

справедливо лишь при $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 0$. Значит, $\Theta = \Theta$ – единственное разложение нулевой матрицы через предложенные матрицы. Тогда ранг данной группы равен 3, то есть rank(F) = = 3. Заметим, что $|F| = 8$. ■

Теорема. Для любого натурального числа n справедлива формула: $|RC_n| = 2^{2n-1}$.

Доказательство. Для группы RC_n справедливо равенство:

$$RC_n = \langle E_1; E_2; \ldots; E_n; E^1; E^2; \ldots; E^n \rangle.$$

Матрицы $E_1, E_2, \ldots, E_n, E^1, E^2, \ldots, E^n$ выражаются друг через друга, точнее, каждая матрица есть сумма всех остальных. В частности,

$$E_1 = E_2 + \ldots + E_n + E^1 + E^2 + \ldots + E^n.$$

Тогда

$$RC_n = \langle E_2; \ldots; E_n; E^1; E^2; \ldots; E^n \rangle.$$

Суммируя любое количество различных матриц из множества $\{E_2; \ldots; E_n; E^1; E^2; \ldots E^n\}$ нулевую матрицу не получаем. Значит, $m(2n-1) = 1$, поэтому $\{E_2; \ldots; E_n; E^1; E^2; \ldots E^n\}$ – ФСО группы RC_n. Отсюда следует, что порядок группы RC вычисляется по формуле 2^{2n-1}.

Заметим, что формула справедлива и в случае $n = 1$, т. к. тогда $RC_1 = \{(0); (1)\}$.

Итак, $|RC_n| = 2^{2n-1}$ для любого натурального числа n. ■

Из теоремы следует, что количество всех различных разложений нулевой матрицы в группе RC_n вычисляется по формуле:

$$m(|RC_n|) = 2^{2^{2n-1} - 2n}.$$

В частности, в группе RC_3, состоящей из 32 матриц, нулевая матрица имеет $2^{26} = 67108864$ разложений.

Список литературы

1. *Каргополов М.И., Мерзляков Ю.И.* Основы теории групп. М., 1982.
2. *Попов И.Н.* Группы *RC* и *RCD*: моногр. Архангельск, 2014.

References

1. Kargopolov M.I., Merzlyakov Yu.I. *Osnovy teorii grupp* [Fundamentals of the Group Theory]. Moscow, 1982.
2. Popov I.N. *Gruppy RC i RCD:* monogr. [Group *RC* and *RCD*: monograph.]. Arkhangelsk, 2014.

Popov Ivan Nikolaevich
Institute of Mathematics, Information and Space Technologies,
Northern (Arctic) Federal University named after M.V. Lomonosov (Arkhangelsk, Russia)

THE NUMBER DECOMPOSITIONS OF MATRICES IN THE SUBGROUP OF *RC*

The results of the researches on the group RC_n are outlined in the paper. The elements of the group *RC* are dimension *n* square matrices over the field Z_2, the group operation is the addition of matrices. Any matrix in the finite additive group *RC* has order 2 and it can be represented as a sum of the so-called row-matrices or column-matrices. The range of the row-matrices and the column-matrices generates a carrier of the group element. Every matrix from *RC* has exactly two different carriers.

Every subgroup in *RC* can be considered as a linear span of matrices, which is called a “generator span’. The span can have several sets of generators. Among all forming linear span there are the so-called fundamental systems, through each any span element is expressed in a unique way.

This paper examines the question of the number decompositions of matrices in the subgroup of *RC* defined as a linear span with a certain number of generators. A relation between a number of decompositions of arbitrary matrices with a number of expansions of zero matrix in terms of the generators of the linear span. A theorem which asserts that the number decompositions of the matrix in the subgroup of *RC* is equal to the number of expansions of zero matrix in this subgroup is formulated and proved. A formula to determine the number of all decompositions of zero matrix in an arbitrary subgroup of the *RC* is proposed. The article deals with the issue of a fundamental system of subgroup generators of *RC* and its role in determining the order of the linear span as a subgroup of *RC* and the group *RC*.

Keywords*: the order of the group, linear span, fundamental system of generators.*

Контактная информация:
адрес: 163002, г. Архангельск, наб. Северной Двины, д. 17;
e-mail: only-for-you-pi@mail.ru

Рецензент – *Попов В.Н.*, доктор физико-математических наук, доцент, заведующий кафедрой математики института математики, информационных и космических технологий Северного (Арктического) федерального университета имени М.В. Ломоносова