ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 25 МАТЕМАТИКИ Выпуск 4
2018

А. В. Анашкин (Москва, Лаб. ТВП). **О матрице смены базиса конечной примарной абелевой группы.**

В работе используем следующие обозначения. $\mathbb{Z}$ — кольцо целых чисел, $\mathbb{N}$ — множество натуральных чисел, $\mathbb{N} \subset \mathbb{Z}$. Для $n, m \in \mathbb{N}$ через $\mathbb{Z}_{n,m}$ обозначаем множество матриц размера $n \times m$ над $\mathbb{Z}$.

Для $a \in \mathbb{N}$ и $b \in \mathbb{Z}$ то обстоятельство, что a делит b обозначаем $a|b$, а если при $A \in \mathbb{Z}_{n,m}$, $n, m \in \mathbb{N}$, то в случае, когда a делит все элементы матрицы A, используем обозначение $a|A$. При этом, в случае, когда в матрице A есть элемент, который не делится на a, используем обозначение $a \nmid A$.

Для $a, b \in \mathbb{Z}\backslash\{0\}$ через НОД (a, b) обозначаем минимальное $c \in \mathbb{N}$ с условием $c|a$ и $c|b$. Для чисел $r \in \mathbb{N}$, $a \in \mathbb{Z}$ и простого числа p определим число $\|a\|_{p^r}$:

$$\|a\|_{p^r} = \begin{cases} p^r, & p^r|a, \\ \text{НОД}(a, p^r), & p^r \nmid a. \end{cases}$$

Если G — группа, $a, b, c \ldots \in G$, то запись $\langle a, b, c \ldots \rangle = G$ обозначает, что совокупность элементов $a, b, c \ldots$ порождает группу G.

Пусть $(G, +)$ — конечная аддитивная абелева группа примарного порядка p^t, p — простое число, $t \in \mathbb{N}$, с нейтральным элементом 0.

Известно, для группы G существуют и однозначно определены числа $s \in \mathbb{N}$, $t_1, t_2, \ldots, t_s \in \mathbb{N}$, $t_1 < t_2 > \cdots > t_s$, $k_1, \ldots, k_s \in \mathbb{N}$ такие, что $\sum_{i=1}^{s} k_i t_i = t$ и группа G представляется в виде прямой суммы n своих циклических подгрупп:

$$G = G_1^{(1)} \dot{+} G_2^{(1)} \dot{+} \cdots \dot{+} G_{k_1}^{(1)} \dot{+} G_1^{(2)} \dot{+} G_2^{(2)} \dot{+} \cdots \dot{+} G_{k_2}^{(2)} \dot{+} G_1^{(3)} \dot{+} \cdots \dot{+} G_{k_s}^{(s)}, \tag{1}$$

где $G_j^{(i)} < G$ — циклическая подгруппа порядка p^{t_i}, $j = \overline{1, k_i}$, $i = \overline{1, s}$, $n = \sum_{i=1}^{s} k_i$.

Набор пар чисел $((p^{t_1}, k_1), (p^{t_2}, k_2), \ldots, (p^{t_s}, k_s))$, назовем *типом* группы G. При этом, когда будем говорить о группе с заданным значением типа, всегда считаем, что выполняется условие: $t_1 > t_2 > \cdots > t_s$.

Любой упорядоченный набор порождающих элементов конечной абелевой группы G примарного порядка, обладающий свойствами: (а) мощность группы равна произведению порядков всех порождающих элементов и (б) порядок элементов базиса не возрастает с увеличением номера элемента в наборе, будем называть *базисом* этой группы.

Пусть $x_1, x_2, \ldots, x_n$ — образующие подгрупп в (1): $G_1^{(1)} = \langle x_1 \rangle, G_2^{(1)} = \langle x_2 \rangle, \ldots, G_{k_1}^{(1)} = \langle x_{k_1} \rangle, G_1^{(2)} = \langle x_{k_1+1} \rangle, G_2^{(2)} = \langle x_{k_1+2} \rangle, \ldots, G_{k_2}^{(2)} = \langle x_{k_1+k_2} \rangle, \ldots, G_{k_s}^{(s)} = \langle x_n \rangle$.

Согласно введенному определению набор $(x_1, x_2, \ldots, x_n)$ — базис G и, значит, любой элемент $g \in G$ может быть записан в виде:

$$g = \sum_{q=1}^{n} a_q \, x_q$$

при некоторых $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. При этом каждое из чисел a_q, $q = \overline{1,n}$, определено однозначно по модулю порядка элемента x_q. В частности, равенство

$$0 = \sum_{q=1}^{n} a_q\, x_q$$

возможно тогда и только тогда, когда $ord(x_q) | a_q$ при всех $q = \overline{1,n}$, или, что то же самое $\|a_q\|_{ord(x_q)} = ord(x_q)$.

Теорема. *Пусть G — аддитивная абелева группа примарного порядка p^t, p — простое число, $t \in \mathbb{N}$, типа $((p^{t_1}, k_1), (p^{t_2}, k_2), \ldots, (p^{t_s}, k_s))$, $t_1 > t_2 > \cdots > t_s$, $n = \sum_{i=1}^{s} k_i$, набор $(x_1, x_2, \ldots, x_n)$ — базис G, $A = (a_{q'q}) \in \mathbb{Z}_{n,n}$.*

Набор $(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n) \cdot A$ является базисом G тогда и только тогда, когда:

1) $\det A \neq 0 \mod (p)$;

2) $\dfrac{ord(x_{q'})}{ord(x_{q'})} \Big| a_{q'q}$ при всех $1 \leqslant q' < q \leqslant n$.

З а м е ч а н и е 1. Запись $(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n)A$ означает, что для каждого $q \in \overline{1,n} : y_q = \sum_{q'=1}^{n} a_{q'q \cdot x_{q'}}$.

П р и м е р 1. Пусть $G = (\mathbb{Z}_4, +) \times (\mathbb{Z}_2, +)$, $g \in G$, $g = (\alpha, \beta)$, $\alpha \in \{0,1,2,3\}$, $\beta \in \{0,1\}$, $g_1, g_2 \in G$, $g_1 + g_2 = (\alpha_1, \beta_1) + (\alpha_2 \beta_2) = (\alpha_1 + \alpha_2 \mod (4), \beta_1 + \beta_2 \mod (2))$.

Пусть $x_1 = (1,0)$, $x_2 = (0,1)$. (x_1, x_2) — базис G.

Набор (y_1, y_2), где $y_1 = x_1$ и $y_2 = x_1 + x_2$, это система образующих группы G (так как $x_1 = y_1$ и $x_2 = y_2 - y_1 = y_2 + 3y_1$), но не базис ($ord(y_1) = ord(y_2) = 4$, $|G| = 8$). Как нетрудно видеть условия п. 2 теоремы не выполняются: $(y_1, y_2) = (x_1, x_2) \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $2 \nmid a_{21} = (1)$.

П р и м е р 2. В обозначениях предыдущего примера набор (y_1, y_2), где $y_1 = x_1$ и $y_2 = 2x_1 + x_2$, это не только система образующих (так как $x_1 = y_1$ и $x_2 = y_2 + 2y_1$), но и базис группы G.

Перед доказательством теоремы сформулируем и докажем несколько вспомогательных утверждений.

Далее в утверждениях и леммах тип группы G считаем фиксированным и равным $((p^{t_1}, k_1,), (p^{t_2}, k_2), \ldots, (p^{t_s}, k_s))$, при этом $n = \sum_{i=1}^{s} k_s$.

Через E обозначаем единичную матрицу, размер которой определяется контекстом. Кроме этого, через $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ обозначаем естественный эпиморфизм колец ($\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$).

Непосредственно из определений вытекает

Утверждение 1. *Пусть набор $(x_1, x_2, \ldots, x_n)$ — базис G, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ и $g = \sum_{q=1}^{n} a_q \cdot x_q$. Тогда $ord(g) = \max_{q=\overline{1,n}}(ord(a_q x_q))$, причем $ord(a_q x_q) = \frac{ord(x_q)}{\|a_q\|_{ord(x_q)}}$, $q = \overline{1,n}$.*

Следствие. $\forall\, g \in G : ord(g) \leqslant p^{t_1}$.

Д о к а з а т е л ь с т в о. $\forall\, g \in G \;\; \exists\, a_1, a_2, \ldots, a_n \in \mathbb{Z} : g = \sum_{q=1}^{n} a_q x_q$. Тогда

$$ord(g) = \max_{q=\overline{1,n}}(ord(a_q x_q)) = \max_{q=\overline{1,n}} \left(\frac{ord(x_q)}{\|a_q\|_{ord(x_q)}} \right) \leqslant \max_{q=\overline{1,n}}(ord(x_q)) = ord(x_1) = p^{t_1}.$$

З а м е ч а н и е 2. Мы полагаем хорошо известным факт, что $\forall\, g \in G\, ord(g) \| |G|$ и, следовательно, в нашем случае $ord(g) = p^r$, $r = r(g) \in \mathbb{N}$.

Утверждение 2. *Пусть набор $(x_1, x_2, \ldots, x_n)$ — базис G, $y_1, y_2, y_n \in G : G = \langle y_1, y_2, \ldots, y_n \rangle$. Если $ord(y_q) \leqslant ord(x_q)$, $q = \overline{1,n}$, то набор $(y_1, y_2, \ldots, y_n)$ — базис G.*

Доказательство. Очевидно, так как $G = |\langle y_1, y_2, \ldots, y_n\rangle| \leqslant \prod_{q=1}^{n} ord(y_q) \leqslant \prod_{q=1}^{n} ord(x_q) = |G|$. Равенство $|\langle y_1, y_2, \ldots, y_n\rangle| = |G|$ возможно лишь тогда, когда $ord(y_q) = ord(x_q)$, $q = \overline{1,n}$, и, значит, $ord(y_q) = ord(x_{(q')}$, при $1 \leqslant q \leqslant q' \leqslant n$.

Утверждение 3. . *Пусть* $A \in \mathbb{Z}_{n,n}$ *и* $\det A \neq 0 \mod (p)$. *Тогда* $\forall\, h \in \mathbb{N}$ $\exists B, C \in \mathbb{Z}_{n,n} : A \cdot B = E + p^h \cdot C$.

Доказательство. Пусть $\det A \neq 0 \mod (p)$. Тогда $\varphi(\det(A)) \neq 0$, и, значит $\varphi(\det(A))$ обратим в $\mathbb{Z}_p$. А тогда у матрицы $\varphi(A)$ существует обратная в кольце матриц $(\mathbb{Z})_{n,n}$ и, более того, $\varphi(A)^{-1} = \varphi(A)^{r-1}$ для некоторого $r \in \mathbb{N}$. Следовательно, $\varphi(A^r) = \varphi(A))^r = E$. Тогда $\exists C^* \in \mathbb{Z}_{n,n} : A^r = E + p \cdot C^*$.

Индукций по $h \in \mathbb{N}$ покажем, что найдется матрица $C^{(h)} \in \mathbb{Z}_{n,n}$ такая, что:

$$(E + pC^*)^{p^{h-1}} = E + p^h \cdot C^{(h)}. \tag{2}$$

При $h = 1$ равенство тривиально $(C^{1)} = C^*)$. Пусть $h' > 1$, и при всех $h < h'$ найдется матрица $C^{(h)} \in \mathbb{Z}_{n,n}$, для которой равенство (2) является верным. Докажем существование нужной матрицы при $h = n'$.

Имеем $(E + p \cdot C^*)^{p^{h'-1}} = E + p^{h'-1} \cdot C^{(n'-1)}$ для некоторой матрицы $C^{(n'-1)} \in \mathbb{Z}_{n,n}$. Тогда

$$\begin{aligned}
(E + p \cdot C^*)^{p^{h'}} &= (E + p^{h'-1} \cdot C^{(n'-1)})^p = \sum_{i=0}^{p} \binom{p}{i} p^{i(h'-1)} (C^{(h'-1)})^i \\
&= E + \binom{p}{1} p^{h'-1} C^{(h'-1)} + \cdots + \binom{p}{p-1} (p^{h'-1} C^{(h'-1)})^{p-1} + (p^{h'-1} C^{(h'-1)})^p \\
&= E + p^{h'} \left(\left(\sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) p^{(i-1)(h'-1)} \left(C^{(h'-1)}\right)^i \right) + p^{(p-1)(h'-1)-1} \left(C^{(h'-1)}\right)^p \right).
\end{aligned}$$

Поскольку $p \,|\, \binom{p}{i}$ при $i = \overline{1, p-1}$ и величины $(p-1)(h'-1)-1 \geqslant 0$ и $(i-1)(h'-1) \geqslant 0$ при $\overline{1, p-1}$, то в скобках после множителя $p^{h'}$ находится сумма квадратных целочисленных матриц с коэффициентами целыми числами и, значит, $(A^r)^{p^h-1} = (E+p\cdot C^*)^{p^h} = E+p^h\cdot C^{(h)}$ для некоторой матрицы $C^{(h)} \in \mathbb{Z}_{n,n}$. Полагая $B = A^{r\,p^h-1}$ и $C = C^{(h}$, получаем требуемое равенство. Утверждение доказано.

Доказательство теоремы. Пусть набор $(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n) \cdot A$ — базис G. Тогда $\exists B \in Z_{n,n} : (x_1, x_2, \ldots, x_n) = y_1, y_2, \ldots, x_n) \cdot B$ Отсюда следует, что $(x_1, x_2, \ldots, x_n) = y_1, y_2, \ldots, x_n) \cdot A \cdot B$, или, что то же самое, что $A \cdot B = E \cdot C$, где $E, C \in \mathbb{Z}_{n,n}$, при этом $ord(x_q) \mid c_{qq'}$, $q, q' = \overline{1,n}$. Тогда $p \mid C$, или $C = p \cdot C^*$, $C^* \in \mathbb{Z}_{n,n}$.

Значит $\det(\varphi(A \cdot B)) = \det(\varphi(E + p \cdot C^*)) = \det(\varphi(E)) = 1$. С другой стороны $\det(\varphi(A \cdot B)) = \varphi(\det(A \cdot B)) = \varphi(\det(A)) \cdot \varphi(\det(B))$. Следовательно, $\varphi(\det(A))$ — обратимый элемент поля $\mathbb{Z}_p$, т. е. $\det(A) \neq \mod (p)$.

Далее, для каждого $q \in \overline{1,n}$ выполняется равенство $ord(y_q) = ord(x_q)$ и одновременно $ord(y_q) = \max_{q'=\overline{1,n}}(ord(a_{q'q} \cdot x_{q'})) = \max_{q'=\overline{1,n}} \left(\frac{ord(x_q)}{\|a_{q'q}\|_{ord(x_{q'})}}\right)$. Отсюда $ord(x_q) \geqslant \left(\frac{ord(x_q)}{\|a_{q'q}\|_{ord(x_{q'})}}\right)$ или

$$\|a_{q'q}\|_{ord(x_{q'})} \geqslant \frac{ord(x_{q'})}{ord(x_q)}, \qquad q, q' = \overline{1,n}. \tag{3}$$

При $1 \leqslant q \leqslant q' \leqslant n : ord(x_{q'} \leqslant ord(x_q)$ неравенство (3) верно для любой матрицы A. При $1 \leqslant q' < q \leqslant n$ с учетом замечания 2 неравенство (3) равносильно условию 2)

теоремы:

$$\frac{ord(x_{q'})}{ord(x_q)}\Big| a_{q'q}.$$

Пусть теперь $(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n)\cdot A, ,$ и матрица $A,$ обладает свойствами:

1) $\det A \neq 0 \mod (p)$;

2) $\dfrac{ord(x_{q'})}{ord(x_{q'})}\Big| a_{q'q}$ при всех $1 \leqslant q' < q \leqslant n.$

По утверждению 3 найдутся матрицы $B, C \in \mathbb{Z}_{n,n}$ такие, что $A \cdot B = E + p^{t_1} \cdot C,$ $C = (c_{qq'})$. Поскольку $p^{t_1} = ord(x_1) \geqslant ord(x_q),\ \ q = \overline{1,n},$ то $ord(x_q) \mid c_{qq'},\ \ qq' = \overline{1,n},$ и значит $(y_1, y_2, \ldots, y_n) \cdot B = (x_1, x_2, \ldots, x_n) \cdot A \cdot B = (x_1, x_2, \ldots, x_n) \cdot (E + p^{t_1} \cdot C) = (x_1, x_2, \ldots, x_n)$. То есть $\langle y_1, y_2, \ldots, y_n\rangle = G.$

Далее, пусть $q_0 \in \overline{1,n}.$ Имеем

$$ord(y_{q_0}) = \max\limits_{q=\overline{1,n}}\Big(\frac{ord(x_q)}{\|a_{qq_0}\|_{ord(x_q)}}\Big) = \max\left(\max\limits_{q=1,\overline{q_0-1}}\Big(\frac{ord(x_q)}{\|a_{qq_0}\|_{ord(x_q)}}\Big), \max\limits_{q=\overline{q_0,n}}\Big(\frac{ord(x_q)}{\|a_{qq_0}\|_{ord(x_q)}}\Big)\right)$$

$$\leqslant \max\left(\max\limits_{q=1,\overline{q_0-1}}\Big(\frac{ord(x_q)}{\|a_{qq_0}\|_{ord(x_q)}}\Big), \max\limits_{q=q_0,n}(ord(x_q))\right)$$

$$= \max\left(\max\limits_{q=1,\overline{q_0-1}}\Big(\frac{ord(x_q)}{\|a_{qq_0}\|_{ord(x_q)}}\Big), ord(x_{q_0})\right) \leqslant (*).$$

Поскольку $\frac{ord(x_q)}{ord(x_{q_0})} \mid a_{qq_0}$ при всех $1 \leqslant q < q_0,$ то $\frac{ord(x_q)}{ord(x_{q_0})} \leqslant \|a_{qq_0}\|_{ord(x_q)},$ или $\frac{ord(x_q)}{\|a_{qq_0}\|_{ord(x_q)}} \leqslant ord(x_{q_0}),$ и, продолжая неравенство $(*)$, получаем: $(*) \leqslant \max(\max_{q=1,q_0-1}(ord(x_{q_0})), ord(x_{q_0})) = ord(x_{q_0})$. То есть $ord(y_{q_0}) \leqslant ord(x_{q_0}),\ \ q_0 = \overline{1,n}.$ По утверждению 2 набор $(y_1, y_2, \ldots, y_n)$ — базис $G.$ Теорема доказана.

СПИСОК ЛИТЕРАТУРЫ

1. *Глухов М. М.*, *Елизаров В. П.*, *Нечаев А. А.* Алгебра: учебник. СПб.: «Лань», 2015, 608 с.