Доклады Академии Наук СССР
1947. Том LVII, № 7

МАТЕМАТИКА

И. Н. САНОВ

СВОЙСТВО ОДНОГО ПРЕДСТАВЛЕНИЯ СВОБОДНОЙ ГРУППЫ

(Представлено академиком И. М. Виноградовым 10 III 1947)

Изоморфные представления свободных групп матрицами, в частности матрицами второго порядка, известны ([1-3]). Но в этих представлениях берутся матрицы либо с трансцендентными элементами, либо с целыми элементами очень сложной структуры. Оказывается, свободная группа с двумя производящими элементами имеет представление матрицами второго порядка с целыми коэффициентами такое, что коэффициенты их могут быть любыми числами из определенных арифметических прогрессий. Естественно, конечно, что определитель таких матриц должен быть равен 1. Не оговаривая особо, единицу группы обозначаем в дальнейшем 1.

Теорема 1. *Группа* $\mathfrak{G}$, *порожденная двумя матрицами* $a=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ *и* $b=\begin{pmatrix}1&0\\2&1\end{pmatrix}$ *свободная.*

Доказательство. $\mathfrak{G}=\{a, b\}$. Любой элемент $\mathfrak{G}$ можно представить одним из двух типов слов

$$g=a^{\alpha_1}b^{\alpha_2}a^{\alpha_3}b^{\alpha_4}\dots a^{\alpha_r}b^{\alpha_{r+1}}, \tag{1}$$

где может быть $\alpha_{r+1}=0$, а все $\alpha_i\neq 0$, $i\leqslant r$, или

$$g_1=b^{\beta_1}a^{\beta_2}b^{\beta_3}\dots b^{\beta_l}a^{\beta_{l+1}}, \tag{2}$$

где может быть $\beta_{j+1}=0$, а все $\beta_j\neq 0$, $j\leqslant l$.

Покажем, что в группе $\mathfrak{G}$ $g\neq 1$, если только хоть одно $\alpha_i\neq 0$.

Для доказательства этого будем прямоугольную матрицу $m=(1, 0)$ множить справа на отрезки слова g вида $a^{\alpha_1}b^{\alpha_2}a^{\alpha_3}\dots c^{\alpha_i}$, $c=a$ или b, $i=1, 2, \dots, r+1$. Результат обозначим m_i.

Тогда, если $m_{2i}=(k_{2i}, k_{2i-1})$, то $m_{2i+1}=m_{2i}a^{\alpha_{2i+1}}=(k_{2i}, k_{2i+1})$, где

$$k_{2i+1}=k_{2i-1}+2\alpha_{2i+1}k_{2i}, \tag{3}$$

а $m_{2i+2}=(k_{2i+2}, k_{2i+1})$, где

$$k_{2i+2}=k_{2i}+2\alpha_{2i+2}k_{2i+1}. \tag{4}$$

Эти формулы верны и при $i=0$, если обозначить

$$k_0=1, \quad k_{-1}=0. \tag{5}$$

(3) и (4) дают вместе формулу

$$k_{i+1}=k_{i-1}+2\alpha_{i+1}k_i, \quad i=0, 1, \dots, r. \tag{6}$$

Докажем, что ряд целых чисел $k_{-1}, k_0, k_1, k_2, k_3, \ldots, k_r$ возрастает по абсолютной величине, а если $\alpha_{r+1} \neq 0$, то и $|k_{r+1}| > |k_r|$.

Допустим, что при всех $i < s$ верно неравенство

$$|k_i| \geqslant |k_{i-1}| + 1. \tag{7}$$

(5) дает нам, что (7) верно при $s=1$. Тогда применим формулу (6): $k_s = k_{s-2} + 2\alpha_s k_{s-1}$; переходя к абсолютной величине, имеем: $|k_s| > 2|\alpha_s| |k_{s-1}| - |k_{s-2}|$. Если $\alpha_s \neq 0$, то из (7) получаем:

$$|k_s| \geqslant 2|k_{s-1}| - |k_{s-2}| = |k_{s-1}| + |k_{s-1}| - |k_{s-2}| \geqslant |k_{s-1}| + 1,$$

т. е. неравенство (7) сохраняется и при $i=s$, а так как оно верно при $s=1$, то оно верно при любом s.

Последовательное применение (7) дает $|k_i| \geqslant i+1$, это и доказывает наши утверждения. Если элемент $\mathfrak{G}$ имеет вид (2), то, заметив, что $mb^{\beta_1} = m$, мы сведем к первому случаю, если g_1 содержит хотя бы два неисчезающих степенных множителя. Если же $g_1 = b^{\beta_1}$, то, так как $b^{\beta_1} = \begin{pmatrix} 1 & 0 \\ 2\beta_1 & 1 \end{pmatrix}$, $b^{\beta_1} = 1$ тогда и только тогда, если $\beta_1 = 0$. Это полностью доказывает теорему 1.

Теорема 2. *Группа $\mathfrak{G}$, определенная в теореме 1, состоит из всех матриц g вида:*

$$g = \begin{pmatrix} 1+4l & 2k \\ 2f & 1+4h \end{pmatrix}, \tag{8}$$

где l, k, f и h — любые целые числа, выбранные с единственным условием: определитель матрицы g должен быть равен 1.

Доказательство того, что все матрицы группы $\mathfrak{G}$ имеют вид (8), получаем из того, что произведение любых двух матриц вида (8) будет опять матрица такого же типа, а производящие элементы a, b, a^{-1}, b^{-1} группы $\mathfrak{G}$ имеют вид матриц (8).

Обратное: то, что любая матрица (8) входит в группу $\mathfrak{G}$, доказывается немного сложнее. Пусть любая матрица (8) записана так:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad |A| = 1.$$

При умножении и делении матрицы A справа на a^α и b^β результат опять будет матрица типа (8). Это уже оговорено выше.

Может быть $|a_{11}| \geqslant |a_{12}|$. (9)

Если $|a_{11}| = |a_{12}|$, то условие $|A| = 1$ дает, что $|a_{11}| = 1$ и $|a_{12}| = 1$, а это невозможно, так как число a_{12} четное.

Итак, всегда из (9) следует $|a_{11}| > |a_{12}|$,

$$Ab^{\alpha_1} = \begin{pmatrix} a_{11} + 2\alpha_1 a_{12} & a_{12} \\ a_{21} + 2\alpha_1 a_{22} & a_{22} \end{pmatrix},$$

α_1 — целое число.

Если $a_{12} \neq 0$, то α_1 можно выбрать так, что будет

$$|a_{11} + 2\alpha_1 a_{12}| \leqslant |a_{12}|.$$

Знак равенства и здесь невозможен при этом α_1.

$$Ab^{\alpha_1} = \begin{pmatrix} a'_{11} & a_{12} \\ a'_{21} & a_{22} \end{pmatrix} \quad \text{и} \quad |a'_{11}| < a_{12}.$$

Далее,

$$Ab^{\alpha_1}a^{\alpha_2} = \begin{pmatrix} a'_{11} & a_{12}+2\alpha_2 a'_{11} \\ a'_{21} & a_{22}+2\alpha_2 a'_{21} \end{pmatrix}.$$

α_2 можно выбрать так, что снова будет: $|a'_{11}|>|a_{12}+2\alpha_2 a'_{11}|$, и мы пришли к неравенству типа (9), но с меньшим по абсолютной величине коэффициентом a_{11}, так как $|a_{11}|>|a_{12}|>|a'_{11}|$.

Матрицы, получаемые в процессе этих умножений, все типа (8). Действия можно повторять таким образом до тех пор, пока в результате r-го шага не станет $a_{12}^{(r)}=0$. Определители всех матриц равны 1. $a_{11}^{(r)}\equiv 1 \pmod 4$, отсюда $a_{11}^{(r)}=1$, $a_{22}^{(r)}=1$, $a_{21}^{(r)}=2f$ и

$$Ab^{\alpha_1}a^{\alpha_2}b^{\alpha_3}\dots a^{\alpha_{2r}} = \begin{pmatrix} 1 & 0 \\ 2f & 1 \end{pmatrix} = b^f.$$

Отсюда матрица A выражается как произведение степеней a и b, а потому $A \in \mathfrak{G}$.

Замечание. Если $\mathfrak{G}_1$ — группа всех целочисленных матриц второго порядка с определителем единица, то $\mathfrak{G}$ не является нормальным делителем $\mathfrak{G}_1$, но если мы образуем группу

$$\mathfrak{G}' = \left\{\mathfrak{G}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\} = \mathfrak{G} \times \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\},$$

то $\mathfrak{G}'$ является нормальным делителем $\mathfrak{G}_1$. Факторгруппа $\mathfrak{G}_1/\mathfrak{G}'$ изоморфна симметрической группе трех символов. Порядок ее равен 6.

Поступило
10 III 1947

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] В. Л. Нисневич, Матем. сб., **8** (50) : 3, 395 (1940). [2] Д. И. Фукс-Рабинович, Уч. зап. ЛГУ, **55**, 154 (1940). [3] Х. А. Донияхи, Уч. зап. ЛГУ, **55**, 153 (1940).