The conference of young scientists «Pidstryhach readings – 2025»
May 27–29, 2025, Lviv

UDC 512.11

EXTENDED SPECIAL LINEAR GROUP $ESL_3(Z)$, CRITERION OF ROOTS EXISTENCE, ANALYTICAL FORMULAS OF ROOTS IN $SL_2(\mathbb{F})$, $GL_2(\mathbb{F}_p)$.

Ruslan Skuratovskii

Institute of applied mathematics and mechanics of the NASU,
ruslan@imath.kiev.ua

1 Criterion of roots existence in $ESL_3(\mathbb{Z})$

In this research we continue our previous investigation of wreath product normal structure [1]. We generalize the group of unimodular matrices [2] and find its structure. For this goal we propose one extension of the special linear group.

Let $SL_3(\mathbb{Z})$ denotes the special linear group of degree 3 over integer ring.

Definition 1. *The set of matrices*

$$\{M_i : Det(M_i) = \pm 1, M_i \in GL_3(\mathbb{Z})\}$$

forms ***extended special linear group*** *in $GL_3(\mathbb{Z})$ and is denoted by $ESL_3(\mathbb{Z})$.*

Denote a permutation matrix of order 3 by P_3 and the transvection of group $SL_3(\mathbb{Z})$ [3] by tr_{12}. Suppose $D_{123} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ be additional generator extending $SL(3, Z)$ to $ESL(3, Z)$.

Proposition 1. *The generating set of $ESL(3, Z)$ is D_{123}, P_3, tr_{12} and tr_{32}.*

There is another principal case to generate a splittable extension of $SL_3(Z)$ by the additional matrix $D_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ having $\det(D_1) = -1$, but do not centralizing the group $SL_3(Z)$. Based on the above, we conclude that structure of group generated by groups $\langle D_1 \rangle$ and $SL_3(Z)$ or equivalently by $D_1,\ tr_{12},\ tr_{32},\ P_3$ is $\langle D_1 \rangle \ltimes SL_3(Z) \simeq ESL_3(Z)$. If we substitute generator D_{123} instead of D_1 then in terms of new subgroups decomposition in product takes form $\langle D_{123} \rangle \times SL_3(Z) \simeq ESL_3(Z)$, because D_{123} centralize $SL_3(Z)$.

To increase the size of the generating set, we involve the monomial matrix $M_6 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$. Also suppose that $\bar{t}_{12} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

Proposition 2. *The generating set of $ESL_3(\mathbb{Z})$ is M_6, tr_{12}, D_1. The relations in $ESL_3(Z)$: $M_6 t_{12} M_6^{-1} = t_{31}^{-1}$, $M_6 t_{31} M_6^{-1} = t_{23}^{-1}$, $M_6 t_{23} M_6^{-1} = t_{12}^{-1}$, $M_6 t_{13} M_6^{-1} = t_{32}^{-1}$, $M_6 t_{23}^{-1} M_6^{-1} = t_{31}^{-1}$, $M_6^6 = E$, $M_6^3 = -E$. Furthermore we can consider more elegant set of generators $\langle \bar{t}_{12}, M_6 \rangle$.*

As it is studied by us $ESL_3(\mathbb{Z})$ has a structure of semidirect product $SL_3(\mathbb{Z}) \rtimes < \mathbb{D}_1 >$.

In terms of generating set $P_3, t_{12}, t_{32}, D_{123}$ wherein $P_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, main relations are following: $P_3 t_{12} P_3^{-1} = t_{31}$, $P_3 t_{31} P_3^{-1} = t_{23}$, $P_3 t_{13} P_3^{-1} = t_{32}$, $P_3 t_{12} P_3^{-1} = t_{23}$, $P_3^3 = E$.

Let $\lambda_1,\ \lambda_2,\ \lambda_3$ be e.v. of $A \in SL_3[\mathbb{Z}]$ provided $trA = \lambda_1 + \lambda_2 + \lambda_3 = a$, $b = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3$. Let$\chi_A(x) = x^3 - ax^2 + bx - 1$ denotes characteristic polynomial for A. According to Lemma 1 [1] if $B^2 = A$, then $\mu_1 = \sqrt{\lambda_1},\ \mu_2 = \sqrt{\lambda_2},\ \mu_3 = \sqrt{\lambda_3}$, where $\mu_1,\ \mu_2,\ \mu_3$ are e.v. of B. We introduce the following notations $q = \mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3$, $trB = p = \mu_1 + \mu_2 + \mu_3$. Let $\chi_B(x) = x^3 - px^2 + qx - 1$ be characteristic polynomial of B.

Theorem 1. *The square root of a simple matrix $A \in SL_3[\mathbb{Z}]$ belongs to $SL_3[\mathbb{Z}]$ iff*

$$p^4 - 2ap^2 - 8p + a^2 - 4b = 0 \tag{1}$$

is solvable over $p \in \mathbb{Z}$, then square root (up to matrix similarity)

$$\sqrt{A} \in SL_3(Z).$$

Moreover equivalent condition

$$\left.\begin{aligned} q^2 - 2p = b \in \mathbb{Z} \\ p^2 - 2q = a \in \mathbb{Z} \end{aligned}\right\} \quad \textit{(equal to the sign)}$$

holds.

Remark 1. The square root of a simple matrix A belongs to $SL_3[\mathbb{F}_p]$ up to similarity iff

$$p^4 - 2ap^2 - 8p + a^2 - 4b = 0 \tag{2}$$

is solvable over $p \in \mathbb{F}_p$, then square root

$$\sqrt{A} \in SL_3(\mathbb{F}_p).$$

The equivalent system of conditions

If $p = 2$ then each matrix $A \in SL_3(\mathbb{F}_p)$ has square root $\sqrt{A} \in SL_3(\mathbb{F}_p)$.

2 Matrix roots of higher powers

Proposition 3. *If $A, B \in GL_2(\mathbb{F}_p)$ is root of equation $X^3 = A$, then*

$$B = \frac{A + tr(\sqrt[3]{A})\sqrt[3]{\det(A)}}{\left(tr\sqrt[3]{A}\right)^2 - \sqrt[3]{\det(A)}}.$$

In the case $A \in SL_2(\mathbb{F}_p)$ we specify the values of the formula parameters taking into account that $\det(A) = 1$. Let us define sequences $s_n = \operatorname{tr} B\ s_{n-1} + t_{n-1}$ and $t_n = -\det B\ s_{n-1}$ with initial conditions $s_1 = 1, t_1 = 0$, $s_2 = trB$ and $t_2 = -detB$. Now we prove the following lemma.

Lemma 1. *Sequences s_n, t_n satisfy recurrent equation with characteristic polynomial $c(x)$ which is also characteristic polynomial for matrix B.*

Theorem 2. *Let $n \geqslant 3$ and $A \in M_2(\mathbb{F}_p)$. If $A \neq c \cdot E$ for any $c \in \mathbb{F}_p$ and $R = \{B \in M_2(\mathbb{F}_p) \mid B^n = A\}$ set of it's n-th roots, then next inclusion follows:*

$$R \subset \left\{ B \in M_2(\mathbb{F}_p) \middle| B = \frac{A + b\ Q_{n-2}(a,b) \cdot E}{Q_{n-1}(a,b)},\ b^n = \det A\ ,\ P_n(a,b) = \operatorname{tr} A \right\}.$$

Література

1. *Skuratovskii Ruslan, Lysenko S. O.* Extended Special Linear group $ESL_2(F)$ and matrix equations in $SL_2(F)$, $ESL_2(Z)$ and $GL_2(F_p)$. WSEAS TRANSACTIONS on MATHEMATICS DOI: 10.37394/23206.2024.23.68

2. *Amit Kulshrestha and Anupam Singh.* Computing n-th roots in $SL_2(Z)$ and Fibonacci polynomials. *Proc. Indian Acad. Sci.* (Math. Sci.) (2020) 130:31

3. *STEPHEN P. HUMPHRIES.* Generation of Special Linear Groups by Transvections. JOURNAL OF ALGEBRA 9, (1986), pp. 480-495.

КОЗОБРАЖЕННЯ РОЗШИРЕНОЇ ЛІНІЙНОЇ ГРУПИ $ESL_3(Z)$ І КРИТЕРІЙ ІСНУВАННЯ КОРЕНЯ З МАТРИЦІ

Ukrainian annotation