Involutive and minimal generating sets of Extended Special Linear group $ESL_3(\mathbb{Z})$, formulas of roots in $GL_2(\mathbb{F}_p)$, $GL_2(\mathbb{Z})$ and $SL_3(\mathbb{Z})$.

Skuratovskii R.V.
TNU, Kiev, Ukraine
Tavrida National University, Kiev, Ukraine and Institute of Applied Mathematics and Mechanics of NASU ORCID:0000-0002-5692-6123
ruslcomp@gmail.com, skuratovskii.ruslan@tnu.edu.ua

1 Introduction

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. Groups generated by three involutions, two of which are permutable, have long been of interest in the theory of matrix groups [4], for instance such generating set was researched for $SL_2(\mathbb{Z}+i\mathbb{Z})$. But for size of matrix 3 on 3 this is imposable for some groups. We research this question for $ESL_3(\mathbb{Z})$.

An analytical formula of root in $SL(3,\mathbb{Z})$ is found, recursive formula for n-th power root in $SL(2,\mathbb{Z})$ is found too.

We denote iff — necessary and sufficient condition, e.v. — eigenvalue. Let μ_A be minimal polynomial of A.

Recall that matrix A is called semisimple if μ_A is a product of distinct monic irreducible and separable polynomials; if moreover all these irreducible polynomials have degree 1, then A is called split semisimple or diagonalizable.

2 Concept of $ESL_3(\mathbb{Z})$

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 $ESL_3(\mathbb{Z})$.*

By the transvection t_{ij} we mean the sum $E+e_{ij}$, where e_{ij} is a matrix unit with 1 only in intersection of i-th row and j-th column the rest elements are 0. For instance $t_{12} = \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$.

Denote a permutation matrix of order 3 by P_3 and the transvection [5] by tr_{12} of group $SL_3(\mathbb{Z})$. Suppose $D_{123} = \begin{pmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}$ be additional generator extending $SL(3,\mathbb{Z})$ to $ESL(3,\mathbb{Z})$.

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

There is another principal case to generate a splittable extension of $SL_3(\mathbb{Z})$ 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 $SL_3(\mathbb{Z})$. The alternative generator to D_1 is $D_2 = \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}$ as well as $D_3 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix}$.

Based on the above, we conclude that structure of group generated as extension of $SL_3(\mathbb{Z})$ by $\langle D_1\rangle$ is semidirect product

$$\langle D_1\rangle \ltimes SL_3(\mathbb{Z}) \simeq ESL_3(\mathbb{Z})$$

with kernel $SL_3(\mathbb{Z})$.

This group admits such generating sets $\langle D_1,\ tr_{12},\ tr_{32},\ P_3\rangle$, $\langle D_2,\ tr_{12},\ tr_{32},\ P_3\rangle$ and $\langle D_3,\ tr_{12},\ tr_{32},\ P_3\rangle$.

If we substitute generator D_{123} instead of D_1 then in terms of these subgroups (factors) a decomposition in product takes form

$$\langle D_{123}\rangle \times SL_3(\mathbb{Z}) \simeq ESL_3(\mathbb{Z}),$$

because D_{123} centralize $SL_3(\mathbb{Z})$.

To reduce the size of the generating set, we involve the monomial matrix $M_6=\begin{pmatrix}0&1&0\\0&0&1\\-1&0&0\end{pmatrix}$.

Proposition 2. The generating set of $ESL_3(\mathbb{Z})$ is M_6, tr_{12} and D_1. The **minimal generating set** of $ESL_3(\mathbb{Z})$ is $\langle M_6, tr_{12}\rangle$. The relations in $ESL_3(Z)$: $M_6t_{12}M_6^{-1}=t_{31}^{-1}$, $M_6t_{31}M_6^{-1}=t_{23}^{-1}$, $M_6t_{23}M_6^{-1}=t_{12}^{-1}$, $M_6t_{13}M_6^{-1}=t_{32}^{-1}$, $M_6t_{23}^{-1}M_6^{-1}=t_{31}^{-1}$, $M_6^6=E$, $M_6^3=-E$ also relations between transvections $[t_{ij},t_{jk}]=t_{ik}$, **wherein** $i\neq k$, $[t_{ij},t_{kl}]=e$ for $i\neq l$ and $k\neq j$. Here M_6 is denoted the monomial matrix $M_6=\begin{pmatrix}0&1&0\\0&0&1\\-1&0&0\end{pmatrix}$. 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 $\langle P_3, t_{12}, t_{32}, D_{123}\rangle$ wherein $P_3=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$, its relations are the following: $P_3t_{12}P_3^{-1}=t_{31}$, $P_3t_{31}P_3^{-1}=t_{23}^{-1}$, $P_3t_{12}P_3^{-1}=t_{31}$, $P_3t_{12}P_3^{-1}=t_{23}^{-1}$, $P_3^3=E$, $[t_{ij},t_{jk}]=t_{ik}$, **wherein** $i\neq k$, $[t_{ij},t_{kl}]=e$ provided $i\neq l$ and $k\neq j$.

Let $i_{12}=\begin{pmatrix}1&-1&0\\0&1&0\\0&0&1\end{pmatrix}$ and $i_{23}=\begin{pmatrix}1&0&0\\0&1&1\\0&0&-1\end{pmatrix}$, then $i_{12}i_{23}=\begin{pmatrix}1&1&1\\0&1&1\\0&0&-1\end{pmatrix}$. Squaring this matrix we obtain $I_{13}=\begin{pmatrix}1&0&-1\\0&1&0\\0&0&-1\end{pmatrix}$. Multiplying the involution D_1 on this matrix we get the transvection $I_{13}D_3=\begin{pmatrix}1&0&-1\\0&1&0\\0&0&-1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}=t_{13}$. Note that it is possible to express transvection using only two non-commutative involutions. From here we obtain the set of generators $S=\langle D_1, i_{12}, i_{23}, M_6\rangle$. Similarly for $SL_2[\mathbb{Z}]$ generating set is $S'=\langle i_{12}, i_{23}, M_6\rangle$.

By *diagonal matrix involution* i_{kl} we mean matrix having 1 in k,l coordinate 0 on rest of coordinate exclude diagonal. On diagonal this matrix has 1 in all rows except k. For instance $i_{31}=\begin{pmatrix}1&0&0\\0&1&0\\1&0&-1\end{pmatrix}$.

To construct *essentially involutive* generating set we consider a pair of diagonal matrix involutions i_{12} and D_1 then their product $i_{12}D_1=t_{12}$. Similarly, pair D_2 and i_{23} allow us to express the transvection $i_{23}D_2=t_{23}$ as well as D_1 and i_{13} lead us to expression $i_{13}D_1=t_{13}$. Continuing this process we express by product of involutions the rest of transvections $i_{23}D_2=t_{23}$ and $i_{21}D_2=t_{21}$, $D_2i_{32}=t_{32}$, $D_1i_{31}=t_{31}$.

Thus, this involutive generating set S for an arbitrary matrix $A\in SL_3[\mathbb{Z}]$ consists of 8 involutions $S=\langle D_1, D_2, i_{kl} : k\neq l\, and\, 1\leqslant k,l\leqslant 3\rangle$, similar to how the size of the involutive generating set for S_n is $n-1$ transpositions of form $(i,i+1)$.

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 $\chi_B\left(x\right) = x^3 - px^2 + qx - 1$ be characteristic polynomial of B.

Theorem 1. The square root of A belongs to $SL_3\left[\mathbb{Z}\right]$ iff

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

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

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

Moreover equivalent condition

$$\left.\begin{array}{r} q^2 - 2p = b \in \mathbb{Z} \\ p^2 - 2q = a \in \mathbb{Z} \end{array}\right\}$$

holds.

Proof.

$$\left.\begin{array}{r} tr(A) - 2\left(\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right) \in \mathbb{Z} \\ \left(\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right)^2 - 2\left(\mu_1 + \mu_2 + \mu_3\right) \in \mathbb{Z} \end{array}\right\},$$

then

$$\left.\begin{array}{l} \left(\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right)^2 - 2\left(\mu_1 + \mu_2 + \mu_3\right) = b \in \mathbb{Z} \\ p^2 - 2q = a \in \mathbb{Z} \end{array}\right\},$$

Expressing condition on coefficient of $\chi_A\left(x\right)$ we avail of them as follows here

$$\left.\begin{array}{r} q^2 - 2p = b \in \mathbb{Z} \\ p^2 - 2q = a \in \mathbb{Z} \end{array}\right\}.$$

Let $2q = -b + p^2$, thus we eliminate the variable $q = \frac{p^2 - a}{2}$. Its square $q^2 = \frac{a^2 - 2ap^2 + p^4}{4}$.

The substitution $p - \frac{a}{2}$ cancels the cubic term in $q^2 = \frac{a^2 - 2ap^2 + p^4}{4}$, since $\left(p - \frac{a}{2}\right)^4 = p^4 - 4\frac{a}{2}p^3 + 6\frac{a^2}{4}p^2 - 4\frac{a^3}{8}p + \frac{a^4}{2^4}$. This entails

$$p^4 - 2ap^2 - 8p + a^2 - 4b = 0.$$

Remark 1. The square root of A belongs to $SL_3\left[\mathbb{F}_p\right]$ 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

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

Moreover equivalent condition

$$\left.\begin{array}{r} q^2 - 2p = b \in \mathbb{F}_p \\ p^2 - 2q = a \in \mathbb{F}_p \end{array}\right\}$$

holds.

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

2.1 The necessary condition and criterion of equation $X^2 = A$ solvability in $SL_3[\mathbb{Z}]$

Let $A \in SL_3[\mathbb{Z}]$ with e.v. $\lambda_1,\ \lambda_2, \lambda_3$ and assume that exists $B \in SL_3[\mathbb{Z}]$ such that $B^2 = A$.

Theorem 1 Theorem 3. *The square root of A belongs to $SL_3[\mathbb{Z}]$ iff*

$$tr(A) + 2\left[\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right] \ \textbf{is square in}\, \mathbb{Z}, \tag{3}$$

where $\mu_1,\ \mu_2,\ \mu_3$ are eigenvalues of the matrix B and J_A possess a diagonal structure. If A does not possess diagonal J_A then (3) is only the necessary condition.

Since $trA = trB^2$ and $tr(B)^2 = (\mu_1 + \mu_2 + \mu_3)^2$, where μ_i are e.v. of B, then the equality $tr(A) = tr(B)^2 - 2\left[\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right]$ holds. This equation can be brought into the form $tr(A) + 2\left[\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right] = tr(B)^2$. But $tr(B)^2 = (\mu_1 + \mu_2 + \mu_3)^2$ is square over $\mathbb{Z}$ therefore $tr(A) + 2\left[\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3\right]$ must be square too. Furthermore over F_p a value of the symmetric polynomial $\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3 \in \mathrm{F}_p$. Also due to the Lemma 1 we can obtain $\mu_i = \sqrt{\lambda_i}$. The symmetric polynomial $\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3 \in \mathrm{F}_p$ be denoted by P.

Furthermore since $tr(B)^2 - P = \frac{tr(B)^2 + tr(A)}{2}$ then $P = tr(B)^2 - \frac{tr(B)^2 + tr(A)}{2} = \frac{tr(B)^2 - tr(A)}{2}$. And finally, the last value on the right side, we can express as follows $tr(B)^2 = \left(\sum\limits_{i=1}^{3}\sqrt{\lambda_i}\right)^2$.

We will prove that if the Jordan form J_A is diagonalizable, then when condition (1) is satisfied, solutions (roots) of the equation $X^2 = A$ in $SL_3[\mathbb{Z}]$ exist, indeed one of the roots of A will be a diagonal matrix with property $tr(B)^2 = \left(\sum\limits_{i=1}^{3}\sqrt{\lambda_i}\right)^2$ possessing the e. v. $\sqrt{\lambda_i}$, $i = \overline{1, ..., 3}$. Its square is a matrix A' similar to the matrix A, in other words $(B')^2 = A' \sim A$.

3 Matrix roots of higher powers

Proposition. If $B \in SL_2(\mathbb{F}_p)$ is root of equation $X^3 = A$, then

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

where $A \in SL_2(\mathbb{F}_p)$.

Proof 1 *Proof. If $\sqrt[3]{A} \in SL_2(\mathbb{F}_p)$ then we consider Cayley-Hamilton equation (C.H.E.) $A^3 - \mathrm{tr}\,(A)\,A^2 + (\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3)\,A - \det\,(A) = 0$. Note, that* $\mathrm{tr}\,(A)^2 = (\lambda_1 + \lambda_2 + \lambda_3)^2 = \lambda_1^2 + \lambda_2^2 + \lambda_3^2 - (\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3)$.

Consider C.H.E. for A : $dimA = 2$, $A^2 - \mathrm{tr}\,(A)\cdot A + \det\,(A)\cdot 1 = 0$. Multiplying last equation on A admit us obtain the chain of transformation:

$$\begin{aligned} A^3 &= (\mathrm{tr}\,(A)\,A - \det\,(A))\,A = \mathrm{tr}\,(A)\,A^2 - \det\,(A)\,A = \\ &= \mathrm{tr}\,(A)\,(\mathrm{tr}\,(A)\,A - \det\,(A)) - \det\,(A)\,A = \\ &= \mathrm{tr}\,(A)^2 A - \mathrm{tr}\,(A)\det\,(A) - \det\,(A)\,A = \\ &= \left(\mathrm{tr}\,(A)^2 - \det\,(A)\right)A - \mathrm{tr}\,(A)\det\,(A)\,. \end{aligned} \tag{4}$$

By applying substitute matrix $\sqrt[3]{A}$ instead of A we express

$$\sqrt[3]{A} = \frac{A + \mathrm{tr}\left(\sqrt[3]{A}\right)\sqrt[3]{\det A}}{\mathrm{tr}^2\left(\sqrt[3]{A}\right) - \sqrt[3]{\det\,(A)}}. \tag{5}$$

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

Note that $\det\left(\sqrt[3]{A}\right) = \sqrt[3]{\det(A)}$ *because of determinant is homomorphism.*

But $\mathrm{tr}\left(\sqrt[3]{A}\right)$ *is still not computed. From* (4) *we conclude* $A^3 = \left(\mathrm{tr}(A)^2 - \det(A)\right)A - \mathrm{tr}(A)\det(A)$. *Computing a trace from both sides we obtain* $\mathrm{tr}\left(A^3\right) = \mathrm{tr}(A)^3 - 3\det(A)\,\mathrm{tr}(A)$.

We put $\sqrt[3]{A}$ *instead of* A*, then we get* $\mathrm{tr}(A) = \mathrm{tr}\left(\sqrt[3]{A}\right)^3 - 3\sqrt[3]{\det A}\,\mathrm{tr}\left(\sqrt[3]{A}\right)$.

We need to solve $\mathrm{tr}(A) = \mathrm{tr}\left(\sqrt[3]{A}\right)^3 - 3\sqrt[3]{\det A}\,\mathrm{tr}\left(\sqrt[3]{A}\right)$.

We denote $\sqrt[3]{A}$ *by* X *and obtain the equation*

$$X^3 - 3\sqrt[3]{\det(A)}X - \mathrm{tr}(A) = 0.$$

The solvability *of this equation over base field* $\mathbb{F}_p$ *is equivalent to the* existence *of a trace* $\sqrt[3]{A}$ *in the base field.*

Now we consider singular cases:

- $(\ trB)^2 - \det B = 0$, *where* $B = \sqrt[3]{A}$.
  In that case from (5) *we obtain*

  $$A = B^3 = -\mathrm{tr}\,B \det B \cdot E = -(\mathrm{tr}\,B)^3 \cdot E.$$

  From that we can compute $\mathrm{tr}\,B$ *as a root of the equation* $x^3 + \frac{\mathrm{tr}\,A}{2} = 0$.

- *If we consider additional matrix* 2×2, $B \notin SL_2(\mathbb{F})$ *and* $B^3 = 0$, *then it's minimal canceling polynomial is* X^2 *or* X. *By Celly Hamilton equation (C.H.E)* $B^2 - trB \cdot B + \det B \cdot I = 0$, *which leads us to* $trB = 0, \det B = 0$.

Proposition. 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 $s_n = \mathrm{tr}\,B\ s_{n-1} + t_{n-1}$ 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. 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:

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

3.1 Recursive formula of n-th power root in the matrix ring $M_2(\mathbb{F}_p)$

Here and below we denote identity matrix from the matrix ring $M_2(\mathbb{F}_p)$ by I. Here and below, In contrast to the identity matrix from the group $SL(2,\mathbb{Z})$ denoted as E.

Proposition 1 *Let $A \in M_2(\mathbb{F}_p)$. Then it's cube roots $R = \{B \in M_2(\mathbb{F}_p) \mid B^3 = A\}$ can be obtained as follows:*

1. *If $A = 0$, then $R = \{B \in M_2(\mathbb{F}_p) \mid \det B = 0,\ \operatorname{tr} B = 0\}$;*

2. *If $A = c^3 I$, where $c \in \mathbb{F}_p/0$, then $R = \{c \cdot B \in M_2(\mathbb{F}_p) \mid B^3 = I\}$;*

3. *In other cases $R \subset \left\{ B \in M_2(\mathbb{F}_p) \middle| B = \dfrac{A + ab \cdot I}{a^2 - b}\ ,\ b^3 = \det A,\ a^3 - 3ab = \operatorname{tr} A \right\}$.*

Proof 2
1. *If $B^3 = 0$, then it's minimal canceling polynomial is X^2 or X. By Celly Hamilton equation (C.H.E) $B^2 - \operatorname{tr} B \cdot B + \det B \cdot I = 0$, which leads us to $\operatorname{tr} B = 0, \det B = 0$;*

2. *If B is a solution of $X^3 - c^3 \cdot I = 0$, then it's easy to see that $B' = c^{-1} B$ is a solution of $X^3 - I = 0$;*

3. *Consider C.H.E for B:*
$$B^2 - \operatorname{tr} B \cdot B + \det B \cdot I = 0.$$
Multiplying last equation by B we proceed with the following chain of transformations:
$$B^3 = (\operatorname{tr} B \cdot B - \det B \cdot I) \cdot B = \operatorname{tr} B \cdot B^2 - \det B \cdot B = \operatorname{tr} B(\operatorname{tr} B \cdot B - \det B \cdot I) - \det B \cdot B =$$
$$= (\operatorname{tr} B)^2 \cdot B - \operatorname{tr} B \det B \cdot I - \det B \cdot B = ((\operatorname{tr} B)^2 - \det B) \cdot B - \operatorname{tr} B \det B \cdot I.$$
If $(\operatorname{tr} B)^2 - \det B = 0$, then we obtain $A = B^3 = -\operatorname{tr} B \det B \cdot I = (-\operatorname{tr} B)^3 \cdot I$, which leads us to previous cases.

Otherwise $(\operatorname{tr} B)^2 - \det B \neq 0$ and we express B:
$$B = \frac{B^3 + \operatorname{tr} B \det B\ I}{(\operatorname{tr} B)^2 - \det(B)}$$
Now since $B^3 = A$ we conclude $\det A = \det B^3 = (\det B)^3$ and hence $\det B$ is a root of polynomial $x^3 - \det A = 0$.

Last thing remaining is to find $\operatorname{tr} B$.
By computing trace from both sides of $A = ((\operatorname{tr} B)^2 - \det B) \cdot B - \operatorname{tr} B \det B \cdot I$ we get:
$$\operatorname{tr} A = (\operatorname{tr} B)^3 - 3 \operatorname{tr} B \det B$$
From which we conclude that $\operatorname{tr} B$ is a root of $x^3 - 3 \det B \cdot x - \operatorname{tr} A = 0$.

In general case we define complete symmetric polynomial of n-th degree in two variables:
$$h_n(x, y) = \sum_{k=0}^{n} x^k y^{n-k}.$$
In view of the fundamental theorem of symmetric polynomials $\exists!$ polynomial $Q(x, y) \in \mathbb{F}_p[x, y]$, such that: $Q(e_1, e_2) = h_n$, where $e_1 = x + y$, $e_2 = xy$ — elementary symmetric polynomials.

Likewise we determine the power symmetric polynomial of n-th degree in two variables:
$$p_n(x, y) = x^n + y^n.$$
And polynomial $P(x, y) \in \mathbb{F}_p[x, y]$, such that $P(e_1, e_2) = p_n$.

Theorem 2 *Let $n \geqslant 3$ and $A \in M_2(\mathbb{F}_p)$. If $A \neq c \cdot I$ 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:*
$$R \subset \left\{ B \in M_2(\mathbb{F}_p) \middle| B = \frac{A + b\ Q_{n-2}(a, b) \cdot I}{Q_{n-1}(a, b)}\ ,\ b^n = \det A,\ P_n(a, b) = \operatorname{tr} A \right\}$$

Proof 3 *Let $B \in M_2(\mathbb{F}_p)$ be a root of equation $X^n = A$. Also consider it's C.H.E.* $c(X) = X^2 - \operatorname{tr} BX + \det B \cdot I$

Then $X^n \underset{c(X)}{\equiv} s_nX + t_nI$ for some $s_n, t_n \in \mathbb{F}_p$ and since $c(B) = 0$ we have

$$A = s_nB + t_nI. \tag{6}$$

Now we prove the following lemma

Lemma 1 *Sequences s_n, t_n satisfy recurrent equation with characteristic polynomial $c(x)$.*

Proof 4 $X^n = X \cdot X^{n-1} \underset{c(X)}{\equiv} X \cdot (s_{n-1}X + t_{n-1}I) = s_{n-1}X^2 + t_{n-1}X \underset{c(X)}{\equiv} s_{n-1}(\operatorname{tr} BX -$
$- \det B \cdot I) + t_{n-1}X = (s_{n-1} \operatorname{tr} B + t_{n-1})X - s_{n-1} \det B \cdot I$

Or by definition of s_n and t_n:

$$\begin{cases} s_n = \operatorname{tr} B \ s_{n-1} + t_{n-1} \\ t_n = -\det B \ s_{n-1} \end{cases} \tag{7}$$

By summing up first expression multiplied by $\det B$ with the second one multiplied by $\operatorname{tr} B$ we get:

$$\det B \ s_n + \operatorname{tr} B \ t_n = \det B \ t_{n-1}$$

or

$$\det B \ s_n = \det B \ t_{n-1} - \operatorname{tr} B \ t_n$$

Substituting into second equation of (7) we obtain:

$$t_n - \operatorname{tr} B \ t_{n-1} + \det B \ t_{n-2} = 0$$

Since s_n and t_n are linearly dependant it follows that s_n satisfy the same recurrent.

Since $X^1 \underset{c(X)}{\equiv} X + 0 \cdot I$ and $X^2 \underset{c(X)}{\equiv} \operatorname{tr} BX - \det B \cdot I$, we have $s_1 = 1, t_1 = 0, s_2 = \operatorname{tr} B$ and $t_2 = -\det B$.

Consider algebraic closure of $\mathbb{F}_p$ that is $\widehat{\mathbb{F}_p}$. Let λ_1, λ_2 be roots of $c(x)$ in $\widehat{\mathbb{F}_p}$ (eigenvalues of B).

1. *If $\lambda_1 \neq \lambda_2$ and $\lambda_1\lambda_2 = \det B \neq 0$:*

$$s_n = c_1\lambda_1^n + c_2\lambda_2^n, \ t_n = c_1'\lambda_1^n + c_2'\lambda_2^n$$

In cases $n = 1, 2$ for s_n we get:

$$\begin{cases} c_1\lambda_1 + c_2\lambda_2 = 1, \\ c_1\lambda_1^2 + c_2\lambda_2^2 = \operatorname{tr} B \end{cases}$$

Solving the system using Kramer's rule we obtain:

$$c_1 = \frac{\lambda_2^2 - \lambda_2 \operatorname{tr} B}{\lambda_1\lambda_2^2 - \lambda_1^2\lambda_2} = -\frac{1}{\lambda_2 - \lambda_1}, \ c_2 = \frac{\lambda_1 \operatorname{tr} B - \lambda_2^2}{\lambda_1\lambda_2^2 - \lambda_1^2\lambda_2} = \frac{1}{\lambda_2 - \lambda_1}$$

Substituting constants

$$s_n = \frac{\lambda_2^n - \lambda_1^n}{\lambda_2 - \lambda_1} = h_{n-1}(\lambda_1, \lambda_2) \tag{8}$$

In cases $n = 1, 2$ for t_n we get:

$$\begin{cases} c_1'\lambda_1 + c_2'\lambda_2 = 0, \\ c_1'\lambda_1^2 + c_2'\lambda_2^2 = -\det B \end{cases}$$

Solving the system using Kramer's rule we obtain:

$$c_1' = \frac{\lambda_2 \det B}{\lambda_1\lambda_2^2 - \lambda_1^2\lambda_2} = \frac{\lambda_2}{\lambda_2 - \lambda_1},\ c_2' = -\frac{\lambda_1 \det B}{\lambda_1\lambda_2^2 - \lambda_1^2\lambda_2} = -\frac{\lambda_1}{\lambda_2 - \lambda_1}$$

Substituting constants

$$t_n = \frac{\lambda_1^n\lambda_2 - \lambda_1\lambda_2^n}{\lambda_2 - \lambda_1} = -\det B \cdot \frac{\lambda_1^{n-1} - \lambda_2^{n-1}}{\lambda_1 - \lambda_2} = -\det B\ h_{n-2}(\lambda_1, \lambda_2) \tag{9}$$

2. *In general case for each $n \geq 3$ we consider polynomial $D_n(\lambda_1, \lambda_2) = h_{n-1} - \operatorname{tr} B h_{n-2} + \det B h_{n-3}$. It's a continuous function of variables λ_1, λ_2.*

   Previously we proved that $D_n(\lambda_1, \lambda_2) = 0$ if $\lambda_1 \neq \lambda_2$ and $\lambda_i \neq 0$.

   From continuity follows that $D_n(\lambda_1, \lambda_2) = 0\ \forall\lambda_1, \lambda_2$ and hence formulas (8) and (9) are fulfilled $\forall\lambda_1, \lambda_2$.

Now that we have found s_n and t_n we return to equation (1). If $s_n = 0$, then $A = t_n I$ which contradicts conditions of the theorem. Dividing both sides by s_n we get formula

$$B = \frac{A - t_n I}{s_n} = \frac{A + \det B\ h_{n-2}(\lambda_1, \lambda_2) \cdot I}{h_{n-1}(\lambda_1, \lambda_2)} = \frac{A + \det B\ Q_{n-2}(\operatorname{tr} B, \det B) \cdot I}{Q_{n-1}(\operatorname{tr} B, \det B)}$$

The last thing remaining is to express $\det B$ and $\operatorname{tr} B$ in terms of A.
Since $\det A = \det B^n = \det B^n$, $\det B$ can be obtain as root of polynomial $x^n = \det A$.
To find $\operatorname{tr} B$ we compute trace from both sides of $B = \dfrac{A - t_n I}{s_n}$:

$$\begin{aligned} \operatorname{tr} A = \operatorname{tr} B\ s_n + 2\ t_n = \operatorname{tr} B\ h_{n-1}(\lambda_1, \lambda_2) - 2\det B\ h_{n-2}(\lambda_1, \lambda_2) = \\ = h_n(\lambda_1, \lambda_2) - \lambda_1\lambda_2\ h_{n-2}(\lambda_1, \lambda_2) = \lambda_1^n + \lambda_2^n = p_n(\lambda_1, \lambda_2) = P_n(\operatorname{tr} B, \det B). \end{aligned}$$

4 Analytical formula of square root in $SL_3(\mathbb{Z})$.

Let $P = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3$, then $trB^2 - tr(B)^2 = 2P$. Consider the matrix equation

$$X^2 = A.$$

Then solution of previous equation is matrix B defined by the formula:

$$B = \frac{A^2 - \frac{tr(B)+tr(A)^2}{2}A - tr\,(A)}{\left(1 - \frac{tr(B)+tr(A)^2}{2}trA\right)}.$$

The characteristic polynomial $-X^3 + tr\,(B)\,X^2 - PX + E = 0$. Applying Celly Hamilton Theorem for B we have $-B^3 + tr\,(B)\,B^2 - PB + E = 0$. $B^3 = tr\,(B)\,B^2 - PB + E$ Multiplying last equation on B admit us obtain $B^4 = tr\,(B)\,B^3 - PB^2 + B$, Transforming left side of equation we express (Left side of this equation can be brought into the form) $B^4 = tr\left(B\right)\left(tr\left(B\right)B^2 - PB + E\right) - PB^2 + B = B^2\left(tr(B)^2 - P\right) + B\left(1 - \mathrm{Pr}\,t\left(B\right)\right) + tr\left(B\right)$. Taking into account the relation between spectral invariant [5] that is bellow

$$tr(B)^2 - P = tr(B)^2 - \frac{tr(B)^2 - tr\left(B^2\right)}{2} = \frac{tr(B)^2 + tr\left(B^2\right)}{2} = \frac{tr(B)^2 + tr\left(A\right)}{2}.$$

Thus we can state relation between spectral invariants: $tr(A)^2 - P = \frac{tr(B)^2 + tr(A)}{2}$. Substituting this as coefficient of second power of matrix $B^4 = B^2\left(tr(B)^2 - P\right) + B\left(1 - \mathrm{P}\,tr\left(B\right)\right) + tr\left(B\right) = \left(\frac{tr(B)^2 + tr\left(B^2\right)}{2}\right)B^2 + \left(1 - \mathrm{P}\,tr\left(B\right)\right)B + tr\left(B\right)$. It yields the equality $B^4 - \left(\frac{tr(B)^2 + tr\left(B^2\right)}{2}\right)B^2 - tr\left(B\right) = \left(1 - \mathrm{P}\,tr\left(B\right)\right)B$. Taking into account that $B^4 = A^2$ and $B^2 = A$, the last equality entails the formula of the root: $B = \frac{A^2 - \frac{tr\left(B^2\right) + tr(B)^2}{2}A - tr(B)}{(1 - \mathrm{P}\,tr(B))} = \frac{A^2 - \frac{tr\left(B^2\right) + tr(B)^2}{2}A - tr(B)}{\left(1 - \frac{tr\left(B^2\right) + tr(B)^2}{2}trB\right)} = \frac{A^2 - \frac{tr(A) + tr(B)^2}{2}B - tr(B)}{\left(1 - \frac{tr(A) + tr(B)^2}{2}trB\right)}$. Thus, we obtain expression of a root

$$B = \frac{A^2 - \frac{tr(B) + tr(A)^2}{2}A - tr\left(A\right)}{\left(1 - \frac{tr(B) + tr(A)^2}{2}trA\right)}.$$

Список литературы

[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 https://doi.org/10.1007/s12044-020-0559-8.

[3] *Levchuk, D. V.* On generation of the group $PSL_n(Z + iZ)$ by three involutions, two of which commute / D. V. Levchuk, Ya. N. Nuzhin // Journal SFU. Serie Math-Ph. 2008. V. 1, Num. 2. pp. 133–139.

[4] Mazurov, V. D. The Kourovka notebook: Unsolved Problems in Group Theory / Eds. V. D. Mazurov, E. I. Khukhro // Sobolev Institute of Mathematics, Novosibirsk, 2022, Num. 20.

[5] *Klyachko Anton A., Baranov D. V.* Economical adjunction of square roots to groups. Sib. math. journal, Volume 53 (2012), Number 2, pp. 250-257.