Extended Special Linear group $ESL_2(\mathbb{F})$ and matrix equations in $SL_2(\mathbb{F})$, $SL_2(\mathbb{Z})$ and $GL_2(\mathbb{F}_p)$

SKURATOVSKII RUSLAN[1,2,a], LYSENKO S. O.[2]
[1] V. I. Vernadsky Taurida national university
John McCain str., 33, Kiev,
UKRAINE
[2] Interregional academy of personnel management,
Kiev,
UKRAINE
$^{a}ORCiDID : 0000 - 0002 - 5692 - 6123$

Abstract: The problem of roots existence for different classes of matrix such as simple and semisimple matrices from $SL_2(\mathbb{F})$, $SL_2(\mathbb{Z})$ and $GL_2(\mathbb{F})$ are solved.
For this purpose, we first introduced the concept of an extended special linear group $ESL_2(\mathbb{F})$, which is generalisation of the matrix group $SL_2(\mathbb{F})$, where $\mathbb{F}$ is arbitrary perfect field. The group of unimodular matrices and extended symplectic group $ESp_2(\mathbb{R})$ are generalised by us, their structures are found.
Our criterion oriented on a general class of matrix depending of the form of minimal and characteristic polynomials, moreover a proposed criterion holds in $GL_2(\mathbb{F})$, where $\mathbb{F}$ is an arbitrary field. The method of matrix factorisation is outlined.
We show that $ESL_2(\mathbb{F})$ is a set of all square matrix roots from $SL_2(\mathbb{F})$ except of that established in our root existence criterion.

Key-Words: extended special linear group, extended symplectic group, splittable extension, set of squares in matrix group, criterion of square root existing in $SL_2(\mathbb{F}_p)$, relations and group generators, matrix factorization.

MSC: 20G07, 15A24, 20G15, 20G40

Received: March 27 2024. Revised: August 29, 2024. Accepted: September 20, 2024. Published: October 16, 2024.

1 Introduction

One of the main purposes of the work is to find an extension of the group containing all roots from a certain set of elements of $SL_2(\mathbb{F})$ over a fixed field $\mathbb{F}$.

Firstly we introduce the new algebraic group that is $ESL_2(\mathbb{F}_p)$ which contains all solutions of $X^2 = A$ for $A \in SL_2(\mathbb{F}_p)$ excluding some simple matrices A non-satisfying established by us conditions. Thereby the group of unimodular matrices, [1], was generalized by us. This allows us to explore the conditions of matrix equation $X^2 = A$ solvability in $SL_2(\mathbb{F}_p)$ as well as in $GL_2(\mathbb{F}_p)$ and in one of splitting extension of $SL_2(\mathbb{F}_p)$ that is $ESL_2(\mathbb{F}_p)$, [2], [3].

Our statements are also true for these groups over the field $\mathbb{R}$ so it leads us to arguments of discreteness problem, [4], [5], solving in some subgroups of $SL(2, \mathbb{R})$.

The square roots from positive definite matrix $A \in \mathbb{GL}(\mathbb{F})$ with distinct eigenvalues (simple matrix) are investigated in [6], but we consider a more general class of semisimple matrix possessing non-square eigenvalues. We find the criterion when roots from this matrices are in $\mathbb{GL}(\mathbb{F}_p)$. In work, [6], an expression for the root was found through a linear combination of matrices for the case of positive matrices, but in the proof from paragraph 4.2 we derived a matrix algebra containing all the roots from a much wider class of matrices than positive matrices over a fixed field $\mathbb{F}$.

We solve, [2], [3] the problem of root existence for a more general case then in [7], which consists in the whole group $G = SL_2(\mathbb{F}_q)$ because of we do not provide additional condition of splitting. Also the authors considered separately conjugacy classes in $SL_2(\mathbb{F}_q)$, [7], such as: central classes, split regular semisimple classes, non-semisimple classes, anisotropic regular semisimple classes. For each case the criterion of solvability of equation is provided. In the last two cases Bruhat decomposition is applied.

The problems of square root from group element existing in $SL_2(\mathbb{F}_p)$, $SL_2(\mathbb{F}_p)$ and $GL_2(\mathbb{F}_p)$ for arbitrary prime p are solved in this paper. The similar

goal of root finding was reached in the GM algorithm adjoining an n-th root of a generator results in a discrete group for group $SL(2,\mathbb{R})$, but we consider this question over finite field $\mathbb{F}_p$. Well known the Cayley-Hamilton method for computing the square roots of the matrix M^n can give answer of square roots existing over a finite field only after computation of $detM^n$ and some real Pell-Lucas numbers by using Bine formula. Our method gives answer about existing $\sqrt{M^n}$ without exponenting M to n-th power. We use only the trace of M or only the e.v. of M, [8].

Earlier it was considered criterion to be square only for the case $\mathbb{F}_p$ is a field of characteristics not equal 2. We solve this problem even for fields $\mathbb{F}_2$ and $\mathbb{F}_{2^n}$. Any criterion to $g \in SL_2(\mathbb{F}_2)$ be square in $SL_2(\mathbb{F}_2)$ was not found before. In case of field with characteristic 0 there is only the Anisotropic case of group $SL_1(\mathbb{Q})$, where $\mathbb{Q}$ is a quaternion division algebra over k was considered in [7].

The authors of [9], [10], argue that for some matrices in $SL_2(\mathbb{F}_2)$ there are not square root in $SL_2(\mathbb{F}_2)$. Now we find exactly which class of matrices are not quadratic element in $SL_2(\mathbb{F}_2)$ furthermore we make group classification of roots distribution in which root could exist in splittable extension of group $SL_2(\mathbb{F}_p)$ over the same field viz it is in $ESL_2(\mathbb{F}_p)$. Furthermore we find a characterisation of matrices $SL_2(\mathbb{F}_2)$ having not square root in any group extension. We investigate root distribution of $A \in SL_2(\mathbb{F}_p)$ by cosets of $ESL_2(\mathbb{F}_p)$ by the normal subgroup $SL_2(\mathbb{F}_p)$.

Thereby we find answer of Waring problem, [11], in $SL_2(F)$ for the image of the word map from G^m to G induced by w, with a generalization of m to fraction of form $\frac{1}{2}$ which be continue in our next work to $\frac{1}{m}$.

The action of subgroup of new group $ESL_2(\mathbb{F}_p)$ introduced here also arose without description of group structure and generators in the topology. Namely, if G is a Morse-Bott foliation on the solid Klein bottle K into 2-dimensional Klein bottles parallel to the boundary and one singular circle S^1 then such group appears as leaf preserving diffeomorphisms for foliations G, [12].

In many geometrical groups there are automorphisms preserve hyperbolic distance (hyperbolic metric) and hyperbolic angles, furthermore they may change orientation of space as well as keep it permanent, [13].

In hyperbolic geometry there are groups preserve hyperbolic length, [14], and orientation as well as changes orientation, in particular projective special linear group $PSL_2(\mathbb{R})$ and $SL_2(\mathbb{R})$ possessing changing orientation due to action of $SL_2(\mathbb{R})$ is nonfaithful because of $PSL_2(\mathbb{R})$ is a homomorphic image of $SL_2(\mathbb{R})$ with non-trivial kernel. A proposed by us group $ESL_2(\mathbb{R})$ also preserves hyperbolic length, [14].

One of interesting algorithmic problem of combinatorial group theory was solved by [15]. It was problem of determining for any element $g \in G$ is g a commutator for free nilpotent group N_r of arbitrary rank r with class of nilpotency 2, [15]. The analogous problem can be formulated for $SL_n(\mathbb{F}_q)$, $GL_n(\mathbb{F}_q)$ and $ESL_n(\mathbb{F}_q)$ over a set of squares.

The problem of the solvability of an equation over a group is well known, [16], [17], [18], [3]. We consider the same problem with additional constrains on the solvability of an equation of the form $X^2 = A$ in a group.

Question of root existence in different forms appears in the Purtzitsky-Rosenberger trace minimizing algorithm, [4], [19], it was considered roots and rational powers of one or both generators of non-elementary two generator discrete subgroups of $PSL_2(\mathbb{R})$ found by the GM algorithm. But we solve existing root problem for arbitrary element of $SL_2(\mathbb{F}_p)$.

Our criteria for the roots existence allows to find a way for solution of Warning problem, [20], for the set of matrix from $SL_2(p)$ and for matrix from $\mathbb{G}L_2(F_p)$.

Also such criteria of roots existence for $SL_2(\mathbb{F}_p)$ and $GL_2(\mathbb{F}_p)$ are established. This criterion is a stricter version of the formulated question for group extensions how large an overgroup of a given group must be in order to contain a square root of any element of the initial group G, which was considered in the paper of [16]. Our criterion gives the answer that such extension is $ESL_2(\mathbb{F})$ for $SL_2(\mathbb{F})$.

2 Litrature review

Many linear equation were solved over different groups, [21], [22], but problem of solving non-linear equation is still not closed. One of the approaches to factorization of matrices was proposed in the work, [23]. We select a subset of matrices that satisfy our criterion for the existence of a square or cubic root and propose a new method for quickly factoring a matrix into 2 different factors due to the conditions we found.

Some results about root computation for simple positively defined matrix $A \in \mathbb{GL}(\mathbb{F})$ is investigated in [6], we continue research this question for all kind of matrices from $\mathbb{SL}(\mathbb{F})$ and $\mathbb{GL}(\mathbb{F})$.

The previous researches, [9], [10], claim that some matrices in $SL_2(\mathbb{F}_2)$ have not square root in $SL_2(\mathbb{F}_2)$ in this work we describe these class.

In view of Waring verbal width by square of $\mathbb{SL}_2(\mathbb{F}_q)$ investigation, [11], our criterion for element of $\mathbb{SL}_2(\mathbb{F}_q)$ to be square in $\mathbb{SL}_2(\mathbb{F}_q)$ can be regarded as more rigid condition of Waring type result for $\mathbb{SL}_2(\mathbb{F}_q)$, [11], that every element of $\mathbb{SL}_2(\mathbb{F}_q)$ is a product of two squares which was generalized by [7], on arbitrary field $\mathbb{F}$ of characteristic $\neq 2$.

In contrast of equation regarded in paper, [7], over field k on characteristic $\neq 2$ we stydy the question of root existence over field of arbitrary characteristic.

In the article [24] a 3-element generator set of the unimodular group was proposed, but a minimal generating set of 2 elements and group structure were not found, the relations in the three-element set of generators of this group were not presented too. But we find minimal generating sets and relations for both 2 and 3-generating sets.

The morphism $P_w : \mathbb{SL}_2(Z)\times\mathbb{SL}_2(Z)\to\mathbb{SL}_2(Z)$ generalizing square computation was constructed in [18], and its root equidistribution turns out depends of trace polynomial.

3 Preliminaries

A large number of works devoted to studying the action of matrix from extension of special linear group having elements with determinant ± 1, [12], [25]. Whereas the concept of this group was not introduced and its structure was not established. To show the importance of introducing new group concept and its studying we notice some topological manifolds in which action of $ESL_2(\mathbb{R})$ subgroups appears.

An action of a subgroup of $ESL_2(\mathbb{R})$ appears in leaf preserving diffeomorphism group which is called foliated leaf preserving in Morse-Bott foliation on the solid torus, [25], of simplest Morse-Bott foliations. But this action of diffeomorphisms was defined geometrically by symmetries with respect to meridian and parallel of torus corresponding to level set and infinite shift on torus also corresponding 3 matrices to these elements were given. Indeed Morse-Bott foliation on solid torus, [25], $T = S^{-1} \times D^2$ into 2-tori parallel to the boundary and one singular circle consists of elements presented by matrices with determinant 1 and -1 by author who characterize it as a subgroup of the whole $GL_2(\mathbb{R})$ group [26]. But now we characterize it more precisely as a subgroup of the smaller group $ESL_2(R) < GL_2(R)$. The diffeomorphisms group of this manifold posses the subgroup $\mathcal{G}$ described in the geometrical terms, where the actions of shifts, symmetries relative to a parallel to a meridian appear, where shift is generated by $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ which is called by reflection. Symmetries relative to a parallel and a meridian are defined by matrices $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ correspondingly. This matrices generate group $\mathcal{G}$ which is a proper subgroup of $ESL_2(\mathbb{Z})$.

We denote by e.v. — **eigenvalue**s. Let μ_A be minimal polynomial of A.

A polynomial $P(X)$ over a given field K is said to be *separable* if its roots are distinct in an algebraic closure of K, that is, the number of distinct roots is equal to the degree of the polynomial.

Simple matrix is a matrix such that characterstic polynomial is separable.

Recall that matrix A is called **semisimple** if μ_A is a product of distinct monic irreducible and separable polynomials, this is equivalent to the minimal polynomial of T being square-free. If moreover all these irreducible polynomials have degree 1, then A is called split semisimple or diagonalizable, [20], [26], [27], [28].

We denote iff — necessary and sufficient condition, e,v. — eigenvalue.

4 Concept of new group

4.1 Definition of new group $ESL_2(\mathbb{R})$

Define the algebraic properties and structures of $ESL_2(\mathbb{F}_p)$ in this item.

Definition 1. *The set of matrices*

$$\{M_i : Det(M_i) = \pm 1, M_i \in GL_2(\mathbb{F}_p)\} \quad (1)$$

*forms **extended special linear group** in $GL_2(\mathbb{F}_p)$ and is denoted by $ESL_2(\mathbb{F}_p)$.*

We establish that, $ESL_2(\mathbb{F}_p) \cong SL_2(\mathbb{F}_p) \rtimes \mathbb{C}_2$, where $\mathbb{C}_2$ is generated by reflection $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. The involution from the top-subgroup $\mathbb{C}_2 \simeq \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ induces the involutive homomorphism in $Aut\,(SL_2(\mathbb{F}_p))$ by action of conjugation.

It is obviously that $ESL_2(\mathbb{F}_p)$ possess presentation in $GL_2(\mathbb{F}_p)$ by matrices described in Definition (1) to show it we establish the homomorphism ψ from $SL_2(\mathbb{F}_p) \rtimes \mathbb{C}_2$ to $ESL_2(\mathbb{F}_p)$. We construct ψ sending elements of the semidirect product containing matrix i as an element of top group $\mathbb{C}_2$ in quotient class of ${}^{ESL_2(\mathbb{F}_p)}\!/_{SL_2(\mathbb{F}_p)}$ having determinant -1 and an with matrix E in the quotient class having determinant 1.

Matrices with determinant -1 correspond to the elements changing Euclidean space base orientation. As it was found in our study of the roots in matrix groups, solutions of $X^2 = A$ arise in defined above group $ESL_2(\mathbb{F}_p)$, where $A \in SL_2(\mathbb{F}_p)$.

We can spread the definition of $ESL_2(\mathbb{F}_p)$ on case of matrices over the arbitrary field $\mathbb{F}$ as well as over the ring $\mathbb{Z}$ and obtain new groups $ESL_2(\mathbb{F})$, $ESL_2(\mathbb{Z})$.

Justification of $SL_2(\mathbb{F}_p)$, $SL_2(\mathbb{Z})$ extensions existence is based on the description $Aut\,(SL_2((\mathbb{F}_p))\,, Aut\,(SL_2(\mathbb{Z}))$ and its subgroups of order 2. In similar way we can extend $SL_n(\mathbb{F})$ to $ESL_n(\mathbb{F})$.

$SL_2(\mathbb{F}_p)$ is of index 2 in $ESL_2(\mathbb{F}_p)$ so its normality is established.

As well known the group of outer automorphisms of $SL_n(\mathbb{Z})$ is semidirect products of the form $SL_n(\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}$ and its isomorphism type depends only on $[\varphi] \in Out(SL_n(\mathbb{Z}))$. Since $Aut(SL_2(\mathbb{Z}))$ contains an element of order 2 that is t^2 therefore homomorphism from top group that is cyclic group $\mathbb{C}_2 =< i >$ of order 2 in $Aut(SL_2(\mathbb{Z}))$ exists.

The existence of a non-trivial homomorphism $\varphi : \mathbb{Z}_2 \to Aut\,(SL_2(\mathbb{Z}))$, as well as $\phi : \mathbb{Z}_2 \to Aut\,(SL_2(\mathbb{F}_p))$ can be proved by indicating an element of order 2 in the automorphisms of base group that is the kernel of the semidirect product we want to construct. There is countergradient automorphism in $SL_2\,(\mathbb{Z})$ that is $\varphi : M \to \left(M^T\right)^{-1}$ or alternating automorphism of order 2 acting by conjugating $\varphi : M \to D^{-1}MD$, where $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and is called by diagonal automorphism, [29], [30]. Also as it is proved in Theorem 2, [24], every automorphism of $SL_2\,(\mathbb{Z})$ is inner automorphism $AXA^{-1}, X \in SL_2\,(\mathbb{Z})$ or inner automorphism AXA^{-1} multiplied on $+E$ or $-E$ in dependence of sum of X generators powers. Thus inner automorphism of order 2 in $SL_2\,(\mathbb{Z})$ as well as in $SL_2\,(\mathbb{F}_p)$ always exists. One of the **generating sets** of $ESL_2(\mathbb{Z})$ has generators $t_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $t_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $t_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. These generators satisfy the relations $t_2^4 = E, t_3^2 = E, (t_2t_3)^2 = E, (t_3t_1)^2 = E$.

Recall the **definition** of **TI − subgroup**, [31], [32]. Let G be a group and $A < G$, then A is called **TI**−subgroup iff $A \cap A^g = e$ for each $g \in G \setminus N_G(A)$.

Remark 1. *Subgroup $\mathbb{C}_2$ is* **TI − subgroup** *but not antinormal subgroup.*

Proof. In view of $\mathbb{C}_2$ is one generated then its centralizer coincides with its normalizer. One easy can verify that the centralizer consists of all diagonal matrices from $ESL_2(\mathbb{F}_p)$. Let us find a structure of such normalizer $N_{ESL_2(\mathbb{F}_p)}(\mathbb{C}_2)$. In view of e.v. of each element of diagonal matrix algebra over field has e. v. $(1,0)^T$ and $(0,1)^T$ then these e. v. are invariant under conjugation by non-singular matrix from the normalizer of top subgroup $\mathbb{C}_2$ in $ESL_2(\mathbb{F}_p)$ is the subgroup consisting of all diagonal matrices from $ESL_2(\mathbb{F}_p)$ and permutational (monomial) matrix $\mathcal{P} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Note that $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ is invariant relatively to conjugations by $\mathcal{P}$ and subgroup of diagonal matrix denoted by $D_2(ESL_2(\mathbb{F}_p))$ of $SL_2(\mathbb{F}_p)$. Therefore the normalizer has structure $N_{ESL_2(\mathbb{F}_p)}(\mathbb{C}_2) \simeq D(ESL_2(\mathbb{F}_p)) \rtimes \mathcal{P}$, where $D(ESL_2(\mathbb{F}_p))$ diagonal subgroup of $ESL_2(\mathbb{F}_p)$.

For the rest of elements condition of $A \cap A^g = e$ for each $g \in ESL_2(\mathbb{F}_p) \setminus N_{ESL_2(\mathbb{F}_p)}(\mathbb{C}_2)$ holds. Thus, $\mathbb{C}_2$ is **TI − subgroup**, but not antinormal subgroup. □

It is obviously that there is a homomorphism in matrix presentation of $ESL_2(\mathbb{F}_p)$ from the semidirect product defining the extension of the group $SL_2(\mathbb{F}_p)$ as the kernel of the semidirect product, by a group of two matrices, one E the second reflection matrix i inducing changes in the sign of the determinant in $ESL_2(\mathbb{F}_p)$.

$SL_2(\mathbb{Z})$ is a normal subgroup of $ESL_2(\mathbb{Z})$, as being the kernel of the determinant, which is a group homomorphism whose image is the multiplicative group $\{-1, +1\}$.

Remark 2. *It is obviously that orthogonal group $O_2(k) < ESL_2(k)$, where k is a field but $O_2(k) \not\lhd ESL_2(k)$, [26], [27].*

Proof. In fact, the action by conjugation of $ESL_2(k)$ does not preserve angles and does not fixe non-degenerate quadratic and Hermitian forms. □

We denote a matrix of shift $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ by s and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ as r they generate $SL_2\,(\mathbb{Z})$, new generator $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ is denoted by i.

Proposition 3. *The group $ESL_2(\mathbb{F}_p) = \langle s, r, i\rangle$ has the following representation:*

$$ESL_2(\mathbb{F}_p) = \langle s, r, i | s^p = e,\ s^{\frac{p+1}{2}} i s^{\frac{p+1}{2}} = i,$$
$$isi^{-1} = s^{-1},\ iri^{-1} = r^{-1},\ r^4 = i^2 = e,\ (sr)^3 = e.\rangle$$

The representation of $ESL_2(\mathbb{Z}) = \langle s, r, i\rangle$ is somewhat simpler:

$$ESL_2(\mathbb{Z}) = \langle s, r, i | isi^{-1} = s^{-1},\ iri^{-1} = r^{-1},$$
$$(sr)^3 = e,\ r^4 = i^2 = e.\rangle$$

Proof. Each relation of $SL_2\,(\mathbb{Z})$ for $r^4 = e$ and $(sr)^3 = e$ holds and is similar to relation in another generators [33], [34] but in [33] the relation $(sr)^3 = e$ among s and r is forgotten. These relations hold in $ESL_2\,(\mathbb{Z})$, because of $SL_2\,(\mathbb{Z})$ is normal subgroup in $ESL_2\,(\mathbb{Z})$. Then new relations are $isi^{-1} = s^{-1}$ and $iri^{-1} = r^{-1}$, the rest of them $r^4 = i^2 = e$ are valid both in $SL_2\,(\mathbb{Z})$ as well as in $SL_2\,(\mathbb{F}_p)$. But taking a step towards studying relations over $\mathbb{F}_3$ we derive a new relations $s^2is^{-1} = i$, $s^3 = E$ which can be generalised for $ESL_2\,(\mathbb{F}_p)$ as $s^{\frac{p+1}{2}} i s^{\frac{p+1}{2}} = i$. The proof is a simple verification of the equalities, for instance

$s^p = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} = E$ in $ESL_2(\mathbb{F}_p)$. The order of s is ∞ in $ESL_2(\mathbb{Z})$, because of s is a shift. Note, that $\mathbb{C}_2 = \langle i \rangle$ and $s^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$.

Thus, the representation of $ESL_2(\mathbb{Z})$ takes form: There are 3 generators s, i, r :

$$s = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, i = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{2}$$

□

Note that the relation $isi^{-1} = s^{-1}$ is characteristic of the **dihedral** groups D_∞ and D_{2p}.

Some interesting relation amongst generators of the kernel subgroup of semidirect product $ESL_2(\mathbb{F}_p) \cong SL_2(\mathbb{F}_p) \rtimes \mathbb{C}_2$ are $r^2 = -E$, $r^{-2}sr^2 = s$.

We briefly introduce the minimal set of generators and relations in $ESL_2(\mathbb{Z})$, [35], i.e. this group over integer ring.

Lemma 4. *The groups $ESL_2(\mathbb{Z})$ and $ESL_2(\mathbb{F}_p)$ have minimal generating set:*

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \tag{3}$$

satisfying the relations

$$P^2 = E, \quad (PL^{-1}PLPL^{-1})^2 = E,$$

and for $ESL_2(\mathbb{F}_p)$ is one more $L^p = E$.

Proof. Note that for $ESL_2(\mathbb{F}_p)$ there is also a relation $L^p = E$.

For proof the statement we show that third generator i from set (2) can be expressed from the considering set (3). This will prove that these 2 elements generate the entire group since the set of generators1 exactly generates the entire group. Note that the inverse element $L^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, is generated as inverse to L belonging to set (3), according to [36], [37].

Then we consider the words in generators of alphabet (3), where $PL^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$, further calculations lead us to $LPL^{-1} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ and $PLPL^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.

With further transformations we obtain $PL^{-1}PLPL^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = i$. And this is the required generator i from initial generating set (2) which, by definition, was equal to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, furthermore now we easy verify the declared in Lemma relation $(PL^{-1}PLPL^{-1})^2 = E$ because $i^2 = E$.

This means that this generator i is expressed through a 2-elements P and L, so these two elements constitute a complete irreducible set of generators. Note that i is matrix corresponding to symmetry having order 2. Therefore the characteristic relation for a dihedral group $iLi^{-1} = L^{-1}$ for L and expressed by us generators i holds.

But third generator r from set 2 for group $ESL_2(\mathbb{Z})$ corresponding to rotation on 90 degree now can be brought into the form $r = iP = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Which completes the proof.

Furthermore the generators L and i form alternating generating set for $ESL_2(\mathbb{Z})$ in view of the fact that the initial set of generators (3) can be expressed from them from them by inverse unfolding of transformations. □

We emphasise that the generator L^{-1} has geometrical sense as the Seifert matrix, [38], and the generator P completes a surgered solid torus shown in Figure 2.7 in [39], to the lens space $L(p, 1)$ by gluing of homeomorphism P to this torus. This confirms geometrical application of presented in Lemma 4 $ESL_2(\mathbb{Z})$.

Remark 5. *The elements P and $PL^{-1}PLPL^{-1}$ forms alternative involutive generators generating set for $ESL_2(\mathbb{Z})$. These generators P and $PL^{-1}PLPL^{-1}$ are similar to reflections of order 2 dihedral group.*

Existence justification of such $SL_2(\mathbb{Z})$ extension by $\mathbb{C}_2$ to $ESL_2(\mathbb{Z}) \cong SL_2(\mathbb{Z}) \rtimes \mathbb{C}_2$ or analogously $SL_2(\mathbb{Z})$ to $ESL_2(\mathbb{F}_p) \cong SL_2(\mathbb{F}_p) \rtimes \mathbb{C}_2$ is based on $Aut(SL_2(\mathbb{Z}))$, [29], [40], [41], structure which is splitting extension $SL_2(\mathbb{Z})$ by $\mathbb{Z}$. As well known the group of outer automorphisms of $SL_n(\mathbb{Z})$ is semidirect products of the form $SL_n(\mathbb{Z}) \rtimes_\varphi \mathbb{Z}$ and its isomorphism type depends only on $[\varphi] \in Out(SL_n(\mathbb{Z}))$. Since $Aut(SL_2(\mathbb{Z}))$ contains an element of order 2 that is t^2 therefore homomorphism from top group that is cyclic group $\mathbb{C}_2 =< i >$ of order 2 in $Aut(SL_2(\mathbb{Z}))$ exists.

The action by right multiplication on $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ of a matrix from $SL_n(\mathbb{Z})$ inducing automorphism in-

verting sing of first column of matrix A. This automorphism invert a sign of $det(A)$.

The **example** of the $ESL_2(\mathbb{F}_3)$ provides us with an exceptional isomorphism with the group of self-combining cubes (full group of Octahedron's symmetries) with inversion about the center. In fact the order of $SL_2(\mathbb{F}_3)$ is $p\left(p^2-1\right)=3\left(3^2-1\right)=24$ therefore the order of $ESL_2(\mathbb{F}_3)$ is 48 withal the group of self-combining of a cube with eversion, equipped with a structure $S_2 \wr S_3$, but as it is also the direct product $S_4 \times C_2 = (A_4 \ltimes C_2) \times C_2$ is of order 48 too.

The group $ESL_2(\mathbb{Z})$, without a structural description and algebraic representation by relations among generators occurs in the topology when the Torelli group which is the kernel of the mapping class group action on the surface M on its first homology group $H_1(M,\mathbb{Z})$, [42], [43], other words the Torelli group is kernel of homomorphism $\mathbf{Mod}_g^b(M) \to Aut(H_1(M,\mathbb{Z})) = SL(2g,\mathbb{Z})$, where g is the genus of M.

In a case when the Torelli group is $SL_2(\mathbb{Z})$ in addition the qoutinet group of action $\mathbf{Mod}_g^b$ on homology classes $H_1(M,Z) = SL(2g,Z)$ that is $Sp_{2g}(\mathbb{Z})$ contains subgroup isomorphic to $\mathbb{Z}_2$ then provided that $\mathbf{Mod}_g^b$ contains subgroup $H \simeq \mathbb{Z}_2$ then there is subgroup in $\mathbf{Mod}_g^b$ having structure of a semidirect product and isomorphic to $ESL_2(\mathbb{Z})$ the correspondent to this subgroup short exact subsequence from item 3.1, [42], splits.

A proper subgroup of $ESL_2(\mathbb{Z})$ appears as geometrical group $\mathcal{G}$, [25], which subgroup in the diffeomorphisms group $D^{lp}(F)$ of T and $[0;\,1]$ on $C^\infty(T,[0;\,1])$ and now be characterized by us in more structural and exact way. Because of the authors, [25], consider $\mathcal{G}$ as subgroup of very wide group $GL(2,\mathbb{Z})$ consisting of matrices for which the vector $(0,1)$ is eigen with eigenvalue ± 1, which was defined as:

$$\mathcal{G} = \left\{ \begin{pmatrix} \varepsilon & 0 \\ m & \delta \end{pmatrix} | m \in \mathbb{Z},\ \varepsilon,\delta \in \{\pm 1\} \right\}.$$

But $\mathcal{G}$ is a proper subgroup of $ESL_2(\mathbb{Z})$ whose structure is studied by us, moreover $ESL_2(\mathbb{Z})$ has a kernel of semidirect product a proper subgroup of $SL_2(\mathbb{Z})$, and $\mathcal{G}$ has in role of kernel a proper subgroup of $SL_2(\mathbb{Z})$, because of $det(\mathcal{G}) = \pm 1$. Furthermore the concept of new group $ESL_2(\mathbb{Z})$ admits us to obtain a structural characterization and set of generators with relations for $\mathcal{G}$. We take in consideration first generator of $\mathcal{G}$ that is involutions generating symmetry of torus with respect to the parallel. It is represented by matrix $t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and generators of the top subgroup of $ESL_2(\mathbb{Z})$ which is denoted by $i = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. One easy can verify that third generator D of $\mathcal{G}$ can be derived from generators of $ESL_2(\mathbb{Z})$ in the following way $t = -E \times i$, because $-E \in ESL_2(\mathbb{Z})$.

Now using concept of new group $ESL_2(\mathbb{Z})$ allows us to give exact and structural characterization of group $\mathcal{G}$ which contains in $D^{lp}(F)$. For this goal we consider subgroup of $ESL_2(\mathbb{Z})$ with kernel $K \simeq \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$. Since $K \simeq \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \simeq \mathbb{Z}$ then $AutK \simeq \mathbb{Z}_2$ and thence homomorphisms from cyclic subgroups $\langle i \rangle$ and $\langle t \rangle$ to $AutK$ exist. One easy can check that $i \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} i^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1}$ and rest of conjugations remain K invariant. Thus, we find a structure of $\mathcal{G}$ which, up to a way to define a semidirect product, is $\mathcal{G} \simeq K \rtimes \langle t,i \rangle$. An important fact that $K \ltimes \langle t,i \rangle$ is a subgroup in $ESL_2(\mathbb{Z})$. Top subgroup of $\mathcal{G}$ has 2 generators but kernel subgroup K is one generated, If we denote $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ then the relations are following $isi = s^{-1},\ tst = s^{-1},\ t^2 = s^2 = e$.

4.2 Some possible applications in topology

Geometrical transformations corresponding to matrices that form the subgroup of the introduced here $SL_2(\mathbb{R}) \rtimes \mathbb{C}_2$ group, occur in leaf preserving diffeomorphism group and vector bundle isomorphism (ξ,η) in Morse-Bott foliation on the solid Klein bottle, [12], (because of matrix A with $det(A) = -1$ changes space orientation as on the Klein bottle), with the complementary circle.

A group of continuous functions implementing rotation $D(y)$, which is a linear isomorphism preserving concentric circles, simultaneously with a shift as standing a second coordinate of tuple, is founded in [12]. Its elements have a form of pair $(we^{2\pi i \lambda_h(s)}, s)$, where $\lambda_h(s)$ ensures sign inversion provided unit shift (on one). We see that this group has structure of semidirect product and denote it by H. Thus, from this group H of diffeomorphisms with additional functions $\lambda_h(s+1) = -\lambda_h(s)$ making changing of sign provided by action of shift on one described in [12], homomorphism in subgroup of $ESL_2(\mathbb{R})$ can be constructed. Homomorphic image can be realized by matrices of rotation with sign inversion inducing by the top group of semidirect product $ESL_2(\mathbb{R})$ that could be also generated by Frobenius normal form $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Thus this subgroup of $ESL_2(\mathbb{R})$ can be embedded in H and this subgroup is realized by

matrices of rotation with sign inversion due to the top group of semidirect product $ESL_2(\mathbb{R})$. One of subgroup of our new group $ESL_2(\mathbb{R})$ is embedded in H. This subgroup has the structure $SO(2) \ltimes \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq: O(2)$. We additionaly denote this subgroup by $\langle \rho \rangle \ltimes \langle i \rangle$.

Previously, a definition of an extended symplectic group was formulated for instance in [44], in terms of this paper a group of extended group is described as group of symplectic matrices with $det(M) = \pm 1$, and denoted by $ESL\left(2, \mathbb{Z}_{\overline{d}}\right)$ on page 4. But its structure was not found.

We define it as the group of symplectic matrices with $\det(M) = \pm 1$ additionally **find its structure** and propose more convenient and usual notification of this group. **Extended symplectic group** be denoted by $ESp_2(\mathbb{R})$ is the group all symplectic matrices such set of matrices having determinant $\det(M) = \pm 1$. Moreover, **extended symplectic group** is subgroup of our group $ESL_2(\mathbb{R})$ and has the structure of semedirect product $ESp_2(\mathbb{R}) \equiv Sp_2(\mathbb{R}) \rtimes \mathbb{C}_2$, where $\mathbb{C}_2$ is defined above, also symplectic group $Sp_2(\mathbb{R})$ is the kernel of the semidirect product. Note that $\mathbb{C}_2$ can be generated not only by i but by matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ too. The justification of established structure is same as for $ESL_2(R)$.

As well known even symplectic group has some applications, [45], [46].

It is obviously that $ESp_2(R) < ESL_2(R)$. We can spread concept of extended symplectic group on ring by considering $ESp_2(\mathbb{Z})$ and $ESp_2(\mathbb{Z}_k)$. Then using finding by us structure

$$ESp_2(\mathbb{Z}_{\overline{d}}) \simeq Sp_2(\mathbb{Z}_{\overline{d}}) \rtimes \mathbb{C}_2$$

we can establish the structure of extended Clifford group more precisely and apply it in Theorem 2, [45], to describe a unique surjective homomorphism from extended Clifford group to group of Clifford operations which was used in [44], in following homomorphism $f_E : \left(Sp_2(\mathbb{Z}_{\overline{d}}) \rtimes \mathbb{C}_2\right) \ltimes \left(\mathbb{Z}_{\overline{d}}\right)^2 \to {}^{EC(d)}/_{I(d)}$ satisfying condition (110) from [45].

In terms and notation of [45], taking into consideration established here structure of $ESL(2, \mathbb{Z})$, the Clifford group in contet of Theorem 2 [45], takes form: $\left(SL\left(2, \mathbb{Z}_{\overline{d}}\right) \rtimes \mathbb{C}_2\right) \ltimes \left(\mathbb{Z}_{\overline{d}}\right)^2$ wherein condition (110) from [45], holds.

Note that group of the diffeomorphisms h coinciding with some vector bundle morphism also function $\lambda_h : \mathbb{R} \to \mathbb{R}$ are described in item 3) of [12], there are subgroup $h'(w, s) = \left(e^{2\pi i \lambda_h(s)}, s\right)$, $\lambda_h(s+1) = -\lambda_h(s)$ presented in form of functions. Now we can describe its structure as semidirect product. We establish a homomorphism from this group to $\langle \rho \rangle \ltimes \langle i \rangle$. Furthermore the top group of $ESL_2(\mathbb{R})$ is the same matrix $i = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ coinciding with a matrix Λ presenting the meridian of torus respect to the parallel, [25].

The subgroup of diffeomorphism $D(L_{p,q})$ of $L_{p,q}$ is under a consideration in [25], whence a group closure of $D(L_{p,q})$ is just $ESL_2(\mathbb{Z})$ but algebraic structure of set was not investigated before so it was classified in [25], as the matrix subset of $GL_2(\mathbb{Z})$ with determinant -1 also there is transformation T in that item with $\det(T) = 1$.

Thus, there are many subgroup of $ESL_2(\mathbb{Z})$ and whole $ESL_2(\mathbb{Z})$ appear in nature but it was not defined and investigated as algebraic group before.

Thus, the surfaces of the thigh and lower leg are on opposite sides of the cutting plane passing through the knee joint. Therefore, to specify a rotation operator in a single basis, you need exactly the operator represented by a matrix from the $ESL_2(\mathbb{R})$ group. By the same reason operators from our group can be applied in geoinformation systems, [47].

5 Criterions of an element root existing in $GL_2(\mathbb{F}_p)$, $SL_2(\mathbb{F}_p)$

5.1 Conditions of root existing in $SL_2(\mathbb{F}_p)$

Let $SL_2(\mathbb{F}_p)$ denotes the special linear group of degree 2 over a finite field of order p. And a degree always means an irreducible character degree in this paper.

We recall the well known relation between eigenvalues of A and $f(A)$.

Lemma 6. *If β is an eigenvalue for B then β^2 is an eigenvalue for B^2.*

Consider the criterion of elements squareness in $SL_2(\mathbb{F}_p)$ as well as in $GL_2(\mathbb{F}_p)$ which can be presented by diagonal matrix. As well known, [27], a matrix can be presented in the diagonal form iff the algebraic multiplicity of its eigenvalues are the same as the geometric multiplicity.

Theorem 7. *Let A be simple diagonalizable or scalar matrix and $A \in SL_2(\mathbb{F})$, [27], then for A there is a solution $B \in SL_2(\mathbb{F})$ of the matrix equation*

$$X^2 = A \tag{4}$$

if and only if

$$\operatorname{tr} A + 2 \tag{5}$$

is quadratic element in $\mathbb{F}$ or 0, where $\mathbb{F}$ is a field.

If $X \in ESL_2(\mathbb{F})$ then the matrix equation (4) *has a solutions iff*

$$\operatorname{tr} A \pm 2 \tag{6}$$

is quadratic element in $\mathbb{F}$ *or 0.*

This solution $X \in ESL_2(\mathbb{F}) \setminus SL_2(\mathbb{F})$ *iff* $(trA-2)$ *is quadratic element or 0 in* $\mathbb{F}$ *but* $(\operatorname{tr} A+2)$ *is not. Conversely* $X \in SL_2(\mathbb{F})$ *iff* $(\operatorname{tr} A+2)$ *is quadratic element. Solutions belong to* $ESL_2(\mathbb{F})$ *and* $SL_2(\mathbb{F})$ *iff* $(\operatorname{tr} A+2)$ *and* $(\operatorname{tr} A-2)$ *are quadratic elements.*

In the case $A \in GL_2(\mathbb{F})$ *this condition* (5) *takes form:*

$$\operatorname{tr} A \pm 2\sqrt{\det A} \tag{7}$$

is quadratic element in $\mathbb{F}$ *or 0 and* $\det A$ *is quadratic element.*

Proof. Throughout the proof a quadraticity of element x or $x=0$ in a field $\mathbb{F}$ be denoted by $\left(\frac{x}{p}\right) \in \{0,1\}$. For concretization, we provide a proof over $\mathbb{F}_p$. But out prove can be spread without changes on *arbitrary field* $\mathbb{F}$ instead $\mathbb{F}_p$.

We assume that matrices A and B have eigenvalues λ_1, λ_2 and μ_1, μ_2 respectively. Let a characteristic polynomial $\chi_B(x)$ of B be the following: $\chi_B(x)=(x-\mu_1)(x-\mu_2)$. We denote $tr(A)$ by a.

Since $det(A), A \in SL_n(\mathbb{F}_p)$ is 1, then eigenvalues of A satisfy the following equality: $\mu_1^2\mu_2^2=1$ that implies $\mu_1\mu_2=\pm 1$. Therefore $a+2\mu_1\mu_2=a\pm 2=(\mu_1+\mu_2)^2$. As is known $tr(B)=\mu_1+\mu_2 \in \mathbb{F}_p$ and $det(B)=\mu_1\mu_2 \in \mathbb{F}_p$. Then according to Lemma 6 a is the sum of the roots μ_1^2, μ_2^2 of a polynomial $\chi_A(x)=(x-\mu_1^2)(x-\mu_2^2)$. Hence $tr(A)=a=\mu_1^2+\mu_2^2=(\mu_1+\mu_2)^2-2\mu_1\mu_2=(tr(B))^2-2$. So, $tr(A)+2=c^2$ for $c=tr(B)$.

In case $\mu_1\mu_2=-1$ we express $tr(A)$ as $tr(A)=a=\mu_1^2+\mu_2^2=(\mu_1-\mu_2)^2-2\mu_1\mu_2=(tr(B))^2+2$ and conclude that $tr(A)-2=c^2$ is quadratic residue in this case. It yields that the solutions $\pm B \in ESL_2(\mathbb{F}) \setminus SL_2(\mathbb{F})$.

We show the existence of $\chi_B(x):=x^2-cx+1$ having roots $\mu_1,\ \mu_2$ which will be the e.v. of B. Let $\chi_{B^2}(x)=\mu^2-a\mu+1$. Then $\mu_1^2,\ \mu_2^2$ are e.v. for A and according to Viet's theorem, $\mu_1^2+\mu_2^2=a$.

Let us prove the sufficiency of the condition $(\frac{\operatorname{tr} A+2}{p})=1$. According to Viet Theorem $\mu_1+\mu_2=c$ and $\mu_1+\mu_2=Tr(B)$, also $c^2=\operatorname{tr} A+2$ by construction of $\chi_B(x)$.

We assume that $\chi_B(x):=x^2-cx+1=(x-\mu_1)(x-\mu_2)$, where $c:=\pm\sqrt{tr(A)+2}$, is characteristic polynomial for B and $\chi_A(x):=x^2-ax+1=(x-\lambda_1)(x-\lambda_2)$, where $a=tr(A)$. To provide justification that $\chi_B(x)$ is characteristic polynomial of $\sqrt{A}$, which denoted by B, we consider $\chi_{B^2}(x)=\left(x-\mu_1^2\right)\left(x-\mu_2^2\right)$ and prove that $\chi_{B^2}(x)=\chi_A(x)$ by showing coinciding of their coefficients. For this goal we have constructed $c^2:=tr(A)+2$, in another hand $c=\mu_1+\mu_2$ and by condition of theorem $tr(A)+2$ is quadratic residue or 0. Consider the sum $\mu_1^2+\mu_2^2=(\mu_1+\mu_2)^2-2\mu_1\mu_2=c^2+2-2\mu_1\mu_2=c^2+2-2=\operatorname{tr} A=a$, according to Viet theorem $\mu_1^2+\mu_2^2$ is coefficient of linear term in χ_{B^2}. The free term of $\chi_{B^2}(x)$ as well as of $\chi_A(x)$ equals to 1 as products of e.v. $\mu_1^2\mu_2^2=Det\left(B^2\right)$ and $\lambda_1\lambda_2=1$ because of $B^2, A \in SL_2(\mathbf{F})$. Thus coefficients of $\chi_{B^2}(x)$ and $\chi_A(x)$ coincide providing an equality of these polynomials. So, their eigenvalues are the same too. Also these eigenvalues are different. Hence these matrices are conjugated.

For the case of generalization on $GL_2(\mathbb{F}_p)$ the proof is the similar but with new absolute term in χ_B. Let $\det A=D$ and $D=d^2$ if $\operatorname{tr} A+2\sqrt{\det A}$ is quadratic element then we construct $\chi_B(x)=x^2-cx+d$, with $d=\pm\sqrt{D}$, then $d^2=\mu_1^2\mu_2^2$, where $\mu_1,\ \mu_2$ are e.v. of B. Consequently $\chi_{B^2}(x)=x^2-\left(c^2-2\right)x+d^2$ in the same time $\chi_A(x)=x^2-tr(A)x+\det(A)$. Thus, these polynomials have the same coefficients, as in case of $SL_2(F_p)$. So B^2 and A are conjugated matrices [48].

Consider *case of scalar matrix* in $\mathbb{G}L_2(\mathbb{F}_p)$. Show that a characteristic polynomial also exists, in view of $c=\operatorname{tr} A-2\sqrt{\det A}=2\lambda-2\sqrt{\lambda^2}=2\lambda\pm 2\lambda$. That is equal to

$$2\lambda\pm 2\lambda=\left[\begin{array}{ll} 0 & \text{iff} \quad \sqrt{\det A}=-\lambda, \\ 4\lambda & \text{iff} \quad \sqrt{\det A}=\lambda. \end{array}\right.$$

The value $4\lambda=\operatorname{tr} A+2\sqrt{\det A}$ is declaimed in the condition (7) as quadratic residue, therefore $4\lambda \in \mathbb{F}_p$. Also absolute term d is $\sqrt{\det A}=\sqrt{\lambda^2}=\pm\lambda \in \mathbb{F}_p$ because of both elements λ on diagonal and rest of elements is 0 moreover all conjugated matrices to a scalar matrix A coincide with A because A in centre, that's why $\lambda \in \mathbb{F}_p$. Thus, the coefficients c, $d \in \mathbb{F}_p$, so such B exists in $SL_2(\mathbb{F}_p)$. In case a *scalar matrix* $A \in \mathbb{S}L_2(\mathbb{F}_p)$ our expression takes form $\operatorname{tr} A-2\sqrt{\det A}=2\pm 2$ whose values are always squares.

In case of diagonal matrix which is not scalar (case of simple matrix) we get $d=\pm\sqrt{\det A}$ but under additional condition to (7) $\det A$ is quadratic residue, hence we have $\pm\sqrt{\det A} \in \mathbb{F}_p$.

The structure of matrix roots B_i of ***exceptional limiting case***, when $\operatorname{tr} A+2=0$ corresponds to a scalar matrix $A=-E$ in $SL_2(\mathbb{F})$, then

$$B_1=\begin{pmatrix} \pm\lambda & 0 \\ 0 & \pm\lambda \end{pmatrix},\ B_2=\begin{pmatrix} 0 & \pm\lambda \\ \mp\lambda & 0 \end{pmatrix},$$

$$B_3=\begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix},\ B_4=\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix},$$

where $\lambda^2 = -1$. It is obviously that this root exists if -1 is quadratic element in $\mathbb{F}$, whence we see B_1, B_2 are elements of $ESL_2(\mathbb{F}_p)$. If $\operatorname{tr} A - 2 = 0$ then we construct the same roots but with condition $\lambda^2 = 1$.

An outstanding case provided by $\lambda^2 = 1$ is Jordan form $J_A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, possess the solutions $S_1 = \begin{pmatrix} \pm 1 & \frac{1}{\pm 2} \\ 0 & \pm 1 \end{pmatrix}$ from $SL_2(\mathbb{F})$ and $G_1 = \begin{pmatrix} \pm\sqrt{\lambda} & \frac{1}{\pm 2\sqrt{\lambda}} \\ 0 & \pm\sqrt{\lambda} \end{pmatrix}$ belonging to $GL_2(\mathbb{F})$.

If $A \in GL_2(\mathbb{F})$ and satisfies (7) then the case $\operatorname{tr} A - 2\sqrt{\det A} = 0$, where $A = \lambda E$ implies that $\operatorname{tr} A = 2\lambda$, and its roots

$$\sqrt{A} = \begin{pmatrix} \pm\lambda & 0 \\ 0 & \pm\lambda \end{pmatrix}, \sqrt{A} = \begin{pmatrix} 0 & \pm\lambda \\ \mp\lambda & 0 \end{pmatrix},$$

$$\sqrt{A} = \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}, \sqrt{A} = \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix},$$

where $\lambda^2 = 1$. Note all roots are conjugated in view of scalar structure of A.

The case $\operatorname{tr} A - 2 = 0$ implies that $A = E$, so its roots

$$\sqrt{A} = \begin{pmatrix} \pm\lambda & 0 \\ 0 & \pm\lambda \end{pmatrix}, \sqrt{A} = \begin{pmatrix} 0 & \pm\lambda \\ \mp\lambda & 0 \end{pmatrix},$$

$$\sqrt{A} = \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix},$$

where $\lambda^2 = 1$.

The sequence of e.v., corresponding to the limiting case ($\lim_{\lambda_i \to 1} (TrA_i + 2) = 0$), is $\lambda_i + \frac{1}{\lambda_i} \to 2$. In this sequence matrices are simple and have diagonal form as well as their roots have limiting form. But the limiting case admits not diagonal structures of roots, where all roots are conjugated i.e. similar matrix. Indeed if A' and A are similar matrix and $(B')^2 = A'$ then $U^{-1}A'U = U^{-1}(B')^2U = U^{-1}B'UU^{-1}B'U = B^2 = A$ so $B = U^{-1}B'U$.

Let us construct the solution of equation $X^2 = A$ in $SL_2(\mathbb{F}_p)$. In a general case we obtain the solution

$$B^2 = A,$$

where $A \sim A'$ with eigenvalues $\lambda_1 = \mu_1^2$, $\lambda_2 = \mu_2^2$. Since $c \in \mathrm{F}_p$ then we can construct in the normal Frobenius form a matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & c \end{pmatrix} = B$$

therefore this matrix is over base field F_p or Q or arbitrary field $\mathbb{F}$. Since $\lambda_1 + \lambda_2 = (\mu_1 + \mu_2)^2 - 2 =$ $\operatorname{tr} A$ and that is why $(\mu_1 + \mu_2)^2 = \operatorname{tr} A + 2$ this equality holds iff $(\frac{\operatorname{tr} A+2}{p}) = 1$. Thus, the condition $(\frac{\operatorname{tr} A+2}{p}) = 1$ is sufficient for existing of $\chi_b(x)$. But it remains to show that these eigenvalues $\sqrt{\lambda_1} = \mu_1$, $\sqrt{\lambda_2} = \mu_2$ are the roots of the characteristic polynomial $\chi_B(x)$.

By the condition of theorem $\operatorname{tr} A + 2$ is a quadratic residue or 0, there is $\sqrt{tr(A) + 2} = \sqrt{(\mu_1 + \mu_2)^2}$ in $\mathrm{F_p}$, whence $tr(\mathrm{B}) \in \mathrm{F_p}$, $\det B \in \mathrm{F_p}$ holds in view of well known theorems, therefore $\chi_B(x)$ has coefficients $c = \sqrt{tr(A) + 2} = \mu_1 + \mu_2$ in $\mathrm{F_p}$, hence B presented in the Frobenius normal form belongs to $SL_2(\mathrm{F_p})$.

Furthermore B having e.v. μ_1, μ_2 is the matrix over $\mathrm{F_p}$, but μ_1, μ_2 can be from $\mathrm{F_{p^2}} \backslash \mathrm{F_p}$. □

Corollary 8. *The condition $(\frac{\lambda_1}{p}) = 1$ and $(\frac{\lambda_2}{p}) = 1$ are necessary over algebraically closed field for diagonalizable non-scalar Jordan form $\sqrt{A} \in ESL_2(F_p)$.*

The condition $(\frac{TrA+2}{p}) = 1$ yields quadraticity of e.v. $\lambda_{1,2}$.

Moreover additional an equality $TrA + 2 = Tr^2B$ holds.

Proof. Proof. In the process of proof we obtain that $\lambda_1 = \beta_1^2$ and $\lambda_2 = \beta_2^2$. Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then in view of $\det B = ad - bc = 1$ and the fact

$$TrA = a^2 + bc + d^2 + bc = a^2 + d^2 + 2bc = a^2 + \\ + d^2 + 2(ad - 1) = a^2 + d^2 + 2ad - 2 = \\ = (a + d)^2 - 2 = Tr^2B - 2.$$

Finally we have $\mathrm{Tr}A + 2 = \mathrm{Tr}^2B$. Thus $\mathrm{Tr}A + 2$ is square so according to Theorem 7 and from diagonal form of A we have $\lambda_1 = \beta_1^2$ and $\lambda_2 = \beta_2^2$. □

Example 9. *Consider Fibonacci matrix $F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ in $SL_2(\mathbb{F}_p)$ then $F^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ which confirms criterion 7 of existing roots in $ESL_2(\mathbb{F}_p)$ because $\operatorname{tr} A - 2 = 1$ because of 1 is square in each field $\mathbb{F}_p$ as well as in $\mathbb{Q}$ and $\mathbb{R}$.*

Next one is $R = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$ in $SL_2(\mathbb{F}_3)$ then $R^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

In another hand we can justify the root existing by criterion for $ESL_2(\mathbb{F}_3)$ because $trR^2 - 2 = 0$.

Example 10. *The case of roots belonging to both cosets of the quotient ${}^{ESL_2(\mathbb{F})}/_{SL_2(\mathbb{F})}$ appears for a matrix A with $tr(A) = 3$ and $\mathbb{F} = \mathbb{F}_{11}$. In fact, in this*

case $tr(A)-2=1$, $tr(A)+2=5$ *one can easily verify that 5 is quadratic residue by* mod11 *because of* $4^2\equiv 5\,(\mathrm{mod}11)$ *and* 1 *is always square.*

Corollary 11. *By the way in the proof of Theorem 7 for simple matrix diagonalizable matrix we obtain additional equality* $trA+2=tr^2B$.

Proof. Let $B=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ then in view of $\det B=ad-bc=1$ and the fact $trA=a^2+bc+d^2+bc=a^2+d^2+2bc=a^2+d^2+2\,(ad-1)=a^2+d^2+2ad-2=(a+d)^2-2=tr^2B-2$. Finaly we have $\mathrm{tr}A+2=\mathrm{tr}^2B$. □

Example 12. *Consider a case when roots are only from* $ESL_2(\mathbb{Z})$, *let* $A=\begin{pmatrix}3 & 2\\ 4 & 3\end{pmatrix}$. *Here* $\mathrm{tr}\,A-2=4$ *that is square, but* $\mathrm{tr}\,A+2=8$ *is not square in* $\mathbb{Z}$. *The square roots*

$$B=\frac{\pm 1}{\sqrt{4}}\begin{pmatrix}2 & 2\\ 4 & 2\end{pmatrix}=\pm\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix},$$

therefore $B\in ESL_2(\mathbb{Z})\setminus SL_2(\mathbb{Z})$.

Corollary 13. *Let* $A\in SL_2(\mathbb{F})$ *and* A *be simple diagonizable matrix satisfying Theorem 7, where* $\mathbb{F}$ *is arbitrary field. Then there exist at most 4 solutions of equation* $X^2=A$ *in* $ESL_2(\mathbb{F})$.

Proof. Let B be solution of $X^2=A$. If $\mathrm{tr}(A)+2$ is quadratic element then we have 2 solutions $\pm B$ in $SL_2(\mathbb{F})$, if $\mathrm{tr}(A)-2$ is such then there are 2 roots $\pm B$ in $ESL_2(\mathbb{F})$. At least if both elements $\mathrm{tr}(A)\pm 2$ are squares in $\mathbb{F}$ then we have 4 roots by the same reasons wherein 2 in $SL_2(\mathbb{F})$ and 2 in $ESL_2(\mathbb{F})$. □

For the case $\mathbb{F}=\mathbb{F}_p$ our criterion can be formulated in terms of Legendre symbol.

Corollary 14. *Let* A *be simple diagonalizable or scalar matrix and* $A\in SL_2(\mathbb{F}_p)$, *[27], then for a matrix* $A\in SL_2(\mathbb{F}_p)$ *there is a solution* $B\in SL_2(\mathbb{F}_p)$ *of the matrix equation*

$$X^2=A \tag{8}$$

if and only if

$$\left(\frac{\mathrm{tr}\,A+2}{p}\right)\in\{0,1\}. \tag{9}$$

If $X\in ESL_2(\mathbb{F}_p)$ *then the matrix equation* (8) *has a solution iff*

$$\left(\frac{\mathrm{tr}\,A\pm 2}{p}\right)\in\{0,1\}. \tag{10}$$

This solution $X\in ESL_2(\mathbb{F}_p)\setminus SL_2(\mathbb{F}_p)$ *iff* $\left(\frac{trA-2}{p}\right)=1$ *or 0, but* $\left(\frac{\mathrm{tr}\,A+2}{p}\right)=-1$. *Conversely* $X\in SL_2(\mathbb{F}_p)$ *iff* $\left(\frac{\mathrm{tr}\,A+2}{p}\right)=1$. *Solutions* $X_i\in ESL_2(\mathbb{F})$ *and* $SL_2(\mathbb{F})$ *iff* $\left(\frac{\mathrm{tr}\,A+2}{p}\right)=1$ *and* $(\mathrm{tr}\,A-2)=1$.

In the case $A\in GL_2(\mathbb{F}_p)$ *this condition* (5) *takes form:*

$$\left(\frac{\mathrm{tr}\,A\pm 2\sqrt{detA}}{p}\right)\in\{0,1\}. \tag{11}$$

The proof is the same as for Theorem 7 but instead of $\mathbb{F}$ we put $\mathbb{F}_p$. But we emphasise that theorems of such a kind, [7], were for algebraic closed field before this paper.

Example 15. *Consider a matrix equation* $X^2=A$ *with e.v. in* $\mathbb{F}_9\backslash\mathbb{F}_3$ *then taking into consideration Corollary 14. It has roots in* $ESL_2(\mathbb{F}_3)\setminus SL_2(\mathbb{F}_3)$ *according to our results, [3]. Let* $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ *since* $\mathrm{tr}\,A+2=2$ *that is non-square residue in* $\mathbb{F}_3$ *but* $\mathrm{tr}\,A-2=-(-1)=1$ *in* $\mathbb{F}_3$, *then according to our criterion and formula for root expression which specialised by us for finite fields and* $SL_2(\mathbb{F}_p)$ *from [10], we use a minus in* $\mathrm{tr}\,A\pm 2$ *i.e.* $\sqrt{A}=\frac{A-E}{\sqrt{\mathrm{tr}\,A-2}}=\frac{1}{\sqrt{\mathrm{tr}\,A-2}}\begin{pmatrix}-0-1, & -1\\ 1, & -0-1\end{pmatrix}=\frac{1}{\sqrt{\mathrm{tr}\,A-2}}\begin{pmatrix}-1, & -1\\ 1, & -1\end{pmatrix}=\begin{pmatrix}-1, & -1\\ 1, & -1\end{pmatrix}=\begin{pmatrix}2, & -1\\ 1, & 2\end{pmatrix}=B$. *Another branch with "-" before the root* $\mathrm{tr}\,A\pm 2$ *lead us to second root:* $\sqrt{A}=\frac{A-E}{-\sqrt{\mathrm{tr}\,A-2}}=\frac{1}{\sqrt{\mathrm{tr}\,A-2}}\begin{pmatrix}-0+1, & 1\\ -1, & -0+1\end{pmatrix}=\frac{1}{\sqrt{\mathrm{tr}\,A-2}}\begin{pmatrix}1, & 1\\ -1, & 1\end{pmatrix}=-B$.

Its $\chi_A(x)=x^2+1=0$ *therefore its roots are* $\pm i\in\mathbb{F}_9\backslash\mathbb{F}_3$ *and* $\pm i$ *are square in* $\mathbb{F}_9$ *that confirms Corollary 14.*

Corollary 16. *If* $A\in GL(\mathbb{F}_2)$ *the condition* (5) *takes the form:*

$$\left(\frac{\mathrm{tr}\,A}{2}\right)\in\{0,1\}.$$

Remark 17. *The formulated criterion for a diagonizable matrix is also true over fields* $\mathbb{Q}$ *and* $\mathbb{R}$.

Proof. The proof is the same only with the change of quadraticity criterion over the new field. □

Corollary 18. *A matrix* A *is square in* $SL_2(\mathbb{F}_{2^k})$ *as well as in* $GL_2(\mathbb{F}_{2^k})$ *iff matrix* A *admits diagonal form over* $\mathbb{F}_{2^k}$.

Furthermore, this condition is sufficient for any square matrix $A \in GL_n F_{2^k}$. If A admits diagonal form over F_{2^k}, then there exists a matrix B over F_{2^k} for which $B^2 = A$. This condition is sufficient even for singular matrix from a matrix ring $M_n(\mathbb{Z})$.

Proof. Firstly we show that square of $B \in SL_2(\mathbb{F}_{2^k})$ having non-diagonal Jordan J_B form is not non-diagonal Jordan form. Let $J_B = \begin{pmatrix} \beta & 1 \\ 0 & \beta \end{pmatrix}$ then $(J_B)^2 = \begin{pmatrix} \beta^2 & 2\beta \\ 0 & \beta^2 \end{pmatrix} = \begin{pmatrix} \beta^2 & 0 \\ 0 & \beta^2 \end{pmatrix} = D_A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$. Besides that square of no one diagonal matrix B does not give non-diagonal Jordan form. Therefore only diagonalizable matrix D_A admits the presence of roots in $SL_2(\mathbb{F}_{2^k})$ this confirms a necessity of the stated condition for $SL_2(\mathbb{F}_{2^k})$.

Let us check the sufficiency of the condition. Indeed, if A is diagonalizable then there exists a non-singular matrix U, for which

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

The elements $\lambda_i,\ i \in \overline{1,...,n}$ belongs to some F_{2^k}. That's why for any $\lambda_i \neq 0$ we have $\lambda_i^{2^k-1} = 1$. So for any $\lambda_i^{2^k} = \lambda_i$, it leads us to replacement D^{2^k} by D. This gives us the equality $A^{2^k} = UD^{2^k}U^{-1} = UDU^{-1} = A$. Since $k \geq 1$, the number 2^k is even. So, we can simply take $B = A^{\frac{2^k}{2}} = A^{2^{k-1}}$. For this B we have $B^2 = A^{2^k} = A$. We will refer e.v. of B as β_1, β_2. In the case $SL_2(\mathbb{F}_2)$ the product of e.v. $\lambda_1\lambda_2 = 1$, wherein $\sqrt{\lambda_1} = \beta_1$, $\sqrt{\lambda_2} = \beta_2$, this imply that the product $\beta_1\beta_2 = \pm 1$. It means that $B \in ESL_2(\mathbb{F}_p)$. Since in F_{2^n} all elements $g_i \in F_{2^n}$ (including eigenvalues $\lambda_1, \lambda_2, \ldots \lambda_n$) are quadratic elements, therefore a diagonal matrix A is always square of the mentioned above B over F_{2^n}. For $M_n(\mathbb{Z})$ the proof is the same.

We exhibit the **formula of roots** of diagonalizible matrices $\sqrt{A} = A^{\frac{x+1}{2}}$, where $x = LCM(ord(\lambda_1), ord(\lambda_2), ..., ord(\lambda_n))$. □

5.2 Conditions of root existing in $GL_2(\mathbb{F}_p)$

Lemma 19. *If e.v. of A lies in the quadratic extension of $\mathbb{F}_p$ i.e. $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, then the matrix algebra $Alg[A] = \langle E,\ A\rangle \simeq F_{p^2}$.*

Proof. We show that the algebra $Alg\,[A] = \langle E, A\rangle$ is isomorphic to the finite field F_{p^2}. As well-known from Galois theory, a quadratic extension of F_p can be constructed by involving of any external element $g \in F_{p^2} \backslash F_p$. For our case, to construct a bijective correspondence with the algebra we put $g = \lambda_1$. We denote this element by g, in particular, for $p = 4m+3$ it may be an element satisfying the relation $g^2 = -1$. Note that the matrix of the rotation by 90 degrees can be used as an example of a matrix A, namely

$$A = \rho_{90} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

satisfies this relation. In case when $p = 4m + 1$ one must construct another matrix instead of ρ_{90} because of $(\frac{-1}{p}) = 1$. It may be a matrix of the form

$$B = \begin{pmatrix} 0 & c \\ -1 & b \end{pmatrix},$$

whose characteristic polynomial $\lambda^2 - b\lambda + c$ is irreducible over $\mathbb{F}_p$.

We define the mapping $\varphi :\ xE + yA \to xe + y\lambda;\ \ a, b \in \mathrm{F}_p$. The mapping φ in $\mathbb{F}_{p^2}$ can be more broadly described, in such a way that a matrix A satisfies $A^2 = -E$, then its e.v. λ is assigned to it in the field F_{p^2}, whereas $\lambda \in F_{p^2} \backslash F_p$, $\varphi :\ y_1A + x_1E \to xe + y\lambda;\ \ x, y \in \mathrm{F}_p$.

Obviously $\det A = 1$, that's why $A \in SL_2(F_p)$ and $\mu_A(x)$ is irreducible because A is semisimple.

According to assumption of this Lemma, the matrix A is semisimple and has no multiple eigenvalues which are not squares in F_p, so $\chi_A(x)$ is irreducible because of definition of semisimple matrix and condition $\lambda_1 \neq \lambda_2$. According to the Lemma about Frobenius automorphism, its eigenvalues are conjugated in F_{p^2}. The method of constructing of $\sqrt{A}$ is the following. Having isomorphism $Alg\,[A] = \langle E, A\rangle \simeq \mathrm{F}_{p^2}$, we set a correspondence $\lambda \leftrightarrow A$ and a correspondence between groups operations in F_{p^2} and $A\lg[A]$. Therefore, solving the equation $(x + \lambda y)^2 = \lambda$ relatively coefficients $x,\ y \in \mathrm{F}_p$ we obtain the coefficients for expression of $\sqrt{A}$, i.e. $\sqrt{A} = x + Ay$. To prove the isomorphism, we establish a bijection between the generators of the algebra $A\lg[A] = \langle E, A\rangle$ and the field F_{p^2}. It is easy to establish in more detail that $A \leftrightarrow \lambda$ and $E \leftrightarrow e$. Also the correspondence between the neutral elements of both structures, i.e. $\varphi(\bar{0}) = 0$ where 0 is the zero matrix. To complete the proof, it remains to show that the kernel of this homomorphism φ is trivial. To do this, we show that among the elements of the algebra there are no identical ones. The surjectivity of φ is obvious.

To show the injectivity, we use a method of proof by contradiction. From the opposite, we assume $y_1A + x_1E = y_2A + x_2E$, $x_i, y_i \in F_p$. Then $y_1A + x_1E = y_2A + x_2E$ it yields that $(y_1 - y_2)\,E =$

$(x_1 - x_2)\, A$, which is impossible since the characteristic polynomial of the matrix A is irreducible but the characteristic polynomial of the identity matrix is reducible. Therefore, our algebra $A \lg [A]$ is isomorphic to the completely linear space of linear polynomials from E and A. In the similar way we prove that polynomial of form $xe + y\lambda$ where $x,\ y \in F_p$ do not repeat. The proof is based on oppositive assumption about coinciding of a two polynomials $x_1 e + y_1 \lambda = x_2 e + y_2 \lambda$ with different coefficients. Then equality $x_1 e + y_1 \lambda = x_2 e + y_2 \lambda$ implies that $(y_1 - y_2)\, \lambda = (x_1 - x_2)\, e$ i.e. $y_1 = y_2$ and $x_1 = x_2$ that contradicts to our assumption. □

Theorem 20. *Let p be prime and $p > 2$. Let a matrix $A \in GL_2(F_p)$ be semisimple with different eigenvalues and let at least one its eigenvalue $\lambda_i \in F_{p^2} \setminus F_p$, $i \in \{1, 2\}$, be **quadratic residue** in F_{p^2} then $\sqrt{A} \in GL_2(F_p)$. Vice-versa is also true.*

As an immediate consequence we get if $detA$ is not quadratic residue in F_p a square root from A does not exist in $GL_2(F_p)$.

Proof. Firstly, we consider the most complex and interesting case when A is not diagonalizable, then $\chi_A(x)$ is irreducible over F_p. By assumption, the matrix is semisimple and its characteristic polynomial is irreducible. So root λ of $\chi_A(x)$ belongs to the quadratic extension of the field F_p. Since each element of F_{p^2} can be presented in form $a + b\lambda,\ \ a, b \in F_p$, then we can construct mapping of matrix algebra generators E and A in generators of F_{p^2} and apply the aforementioned Lemma 19 about isomorphism establish correspondence between property be square in F_{p^2} and in $Alg\,[A] = \langle E, A \rangle$. If one e.v. λ_i is square in F_{p^2} then so is second e.v. because of they are conjugated as roots of characteristic polynomial $\chi_A(x)$ by theorem about Frobenius automorphism (Frobenius endomorphism in perfect field became to be automorphism). Also we construct the mapping $\varphi :\ xE + yA \to xe + y\lambda;\ \ x, y \in \mathrm{F}_p$ establishing isomorphism $Alg\,[A] \simeq F_{p^2}$.

Note, that in order to anlalyze the matrix A, where e.v. are in $\lambda_i \in F_{p^2} \setminus F_p$, we must construct an algebra using matrix A.

If the condition $(\frac{detA}{p}) \in \{0, 1\}$ does not hold then a matrix B satisfying the condition $detB detB = detA$ (where A is not square) does not exist too. □

Example 21. *Consider the square matrix $A = -E$ satisfying conditions of Theorem 20 because of $(\frac{-1}{9}) = 1$ in F_9, provided E is identity matrix in $SL_2(F_3)$. We have to note that there exists the matrix $\begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} = 2I \in SL_2(F_3)$ is the square root for A, where I is the rotation matrix on -90 degrees. Indeed $I^2 = -E$ over F_3.*

Another root of this equation $X^2 = -E$, where A is matrix of elliptic type realizing rotation on 90 degrees $\rho_{90} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = I$ because of $I^2 = -E$, is the matrix of elliptic type.

The matrix $2I$ is the square in $GL_2(F_3)$ because of existence such an element $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^2 = 2\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = 2I$.

Example 22. *Consider the diagonal matrix $A \in GL_2(F_3)$, where $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, emphasizing the need for the condition $(\frac{det(A)}{p}) = 1$ and $\lambda \in F_{p^2} \setminus F_p$ of Theorem 20 for semisimple matrix. Here even the condition $(\frac{det(A)}{p}) = 1$ does not hold as well as $\lambda_{1,2} \notin F_p$ but in $F_{p^2} \setminus F_p$, $A' \in ESL_2(F_3)$. It is easy to verify the absence of root from $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in $GL_2(F_3)$.*

But the matrix $A' = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ satisfying conditions of Theorem 20 has roots $\sqrt{A'} = \pm\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$.

Theorem 23. *Under conditions $(\frac{\lambda}{p}) = 1$ in $\mathbb{F}_p$ and matrix A is similar to a Jordan block of the form*

$$J_A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \tag{12}$$

a square root B of J_A exists in $SL_2(\mathbb{F}_p)$ and takes form $B = \begin{pmatrix} \sqrt{\lambda} & \gamma \\ 0 & \sqrt{\lambda} \end{pmatrix}$, wherein $\gamma = (2\sqrt{\lambda})^{-1}$. The root B belongs to $Alg[A]$ which is described in Lemma 19.

Proof. Assume that a square root from A exists in $SL_2(\mathbb{F}_p)$ or in $ESL_2(\mathbb{F}_p)$ correspondently. We denote a matrix B transformed to upper triangular form by UT_B. Let us show provided that above condition it always exists such $B :\ UT_B^2 = J_A$, where UT_B is B transformed to UTM form. Then we show that it implies existing of solution of $X^2 = A$. From the existence of the Jordan block for A follows the existence of a similarity transformation U transforming B^2 to the Jordan normal form J_B because of $A = B^2$ and A has non-trivial Jordan block denoted by J_A. But a square root from B^2 this operator U transforms in upper triangular form UT_B. Then if we find the solution for

$$UT_B^2 = J_A \tag{13}$$

we can obtain solution for $X^2 = A$ because of the following:

$$A = U \cdot (UT_B)^2 \cdot U^{-1} =$$
$$(U \cdot UT_B \cdot U^{-1})(U \cdot UT_B \cdot U^{-1}) = B^2.$$

It means that such matrix UT_B satisfying previous equation exists and it can be transformed by the same similarity transformation by conjugation in form $UT_B = U^{-1}BU$ by the same matrix that transforms A in J_A because of $B^2 = A$. To show the existing of such solution of (13) we acting by inverse transformation $A = U \cdot (UT_B)^2 \cdot U^{-1} = (U \cdot UT_B \cdot U^{-1})(U \cdot UT_B \cdot U^{-1}) = B^2$, where U is a similarity transformation B to

$$UT_B = \begin{pmatrix} \beta & \gamma \\ 0 & \beta \end{pmatrix}.$$

note that its diagonal elements $b_{11} = b_{22} = \beta$ are the same. Even more easier we can deduce it without applying Lemma 19. We have $b_{11} = b_{22} = \beta$, then $\beta + \beta = \mathrm{Tr}(U^{-1}BU)$. Therefore $2\beta \in \mathrm{F}_p$. It implies that $\beta \in F_p$ if $p > 2$ and

$$(UT_B)^2 = \begin{pmatrix} \beta^2 & 2\beta\gamma \\ 0 & \beta^2 \end{pmatrix}.$$

Here the element γ can be chosen γ : $2\beta\gamma = 1$ so $\gamma = (2\beta)^{-1}$ taking into account that $\beta = \sqrt{\lambda}$ which is already determined by A. Then $(UT_B)^2$:

$$(UT_B)^2 = \begin{pmatrix} \beta^2 & 2\beta\gamma \\ 0 & \beta^2 \end{pmatrix} = \begin{pmatrix} \beta^2 & 1 \\ 0 & \beta^2 \end{pmatrix} =$$
$$= J_A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Furthermore we show that these conditions is also necessary but not only sufficient. It means if $(\frac{\lambda}{p}) = -1$, then there are no matrix B over $SL_2(F_p)$ such that $B^2 = A$. By a reversal of theorem condition and using the representation in the form of UTM for and for we see that B from $PSL_2(F_p)$ such that $B^2 = A$. We see that the eigenvalue of B over lie in the main field — F_p. However, we assumed that $(\frac{\lambda}{p}) = -1$. Thus we obtain the desirable contradiction.

Let us show that condition of non-diagonalizability of matrix is necessary in the conditions of this Theorem. By virtue of the well-known theorem stating that if the algebraic multiplicity is equal to the geometric multiplicity for each eigenvalue, then matrix is diagonalizable otherwise it is not diagonalizable, we see that if the condition of similarity to $J_A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ indicated in this Theorem 23 does not holds, then such A satisfy the conditions of this Theorem 7, where algebraic multiplicity is equal to geometrical. And since the condition 12 of this criterion is nature, therefore, it is no longer necessary to prove the non-diagonalizability condition in Theorem 23.

Proof of **necessity**. Furthermore we show that these conditions is also necessary but not only sufficient. It means if $(\frac{\lambda}{p}) = -1$, then there are no matrix B having non trivial Jordan block over $SL_2(\mathbb{F}_p)$ such that $B^2 = A$. By a reversal of theorem condition and using the representation in the form of UTM for and for we see that B from $SL_2(\mathbb{F}_p)$ such that $B^2 = A$. We see that according to the Lemma the eigenvalue of $B \in SL_2(\mathbb{F}_p)$ correspondingly, lie in the main field – $\mathbb{F}_p$. Furthermore according to Lemma 6 if β is an eigenvalue for B then β^2 is an eigenvalue for B^2, so we have $\beta^2 = \lambda$. However, we assumed that $(\frac{\lambda}{p}) = -1$. Thus we obtain the desirable contradiction. The eigenvalue β has geometrical dimension 1, because of in oppositive case geometrical dim $\beta = 2$ (dimension of eigenvector space of β), then we get that J_B^2 is only scalar matrix B.

The proof is fully completed. □

6 Future research and discussion

The main result of this paper about the criterion of a quadraticity can be extended to larger dimension matrices having a Jordan structure constructed of blocks of dimension 2 or 1. Also, our result for a semisimple matrix of dimension 2 can be generalized to a semisimple matrix of higher dimension.

One new method of matrix factorization, [49], [50], [23] ***due to our square root existence criterions*** can be provided.

If M possesses the presentation $M = A - C$, where $A = B^2$, $C = D^2$, then M can be factorized in the following way $M = (B - D)(B + D)$, provided condition $BD = DB$. For verifying the condition of A, C quadraticity our structural theorems about roots structures are applicable. Theorem 23 outlines the Jordan structure of roots which is key to defining the matrix centralizer.

Indeed, $(B - D)(B + D) = B^2 - D^2 + BD - DB$, whence equality $(B - D)(B + D) = B^2 - D^2$ satisfies if $BD = DB$. Therefore it is important to have quick method of square root existence checking in $SL_2(\mathrm{F})$ also we investigate jourdan structures of matrix roots to obtain an answer about commuting of $\sqrt{A}$ and $\sqrt{B}$. Analogously we can spread the method on case of cubic root existing.

Besides another one new method of matrix factorization for the case If algebra $Alg(A) = \langle E, A \rangle$ is one generated and roots $B_1, B_2 \in Alg(A)$ then B_1, B_2 commutes, because of such algebra is commutative.

It yields some decomposition of A in roots products. Another part of root can be out of $Alg(A)$ in case if $dim(Alg(A)) = 1$.

Such roots $B_1, B_2 \in ESL_2(\mathbb{F}_3)$ always commute if they belongs to one-dimensional algebra $Alg(A) = \langle A \rangle$. Consider $SL_2(\mathbb{F}_3)$ and its element that is the 90 degree rotation matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. For factorization we also use roots of an additional matrix $\sqrt{-A} = B_1 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ and $\sqrt{-A} = B_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Then we can present their product as a factorization of a matrix A

$$A = B_1 B_2 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$ Note that $B_1 = A - E$ that accords with derived us by modification, [3], of Cayley-Hamilton method for roots of matrix of finite field. In general case there are 4 roots possible which are described in [3], therefore more combinations or roots can lead us to grater number of matrix decompositions what can be object of future research.

Consider $SL_2(\mathbb{F}_3)$ and the roots of the - 90 degree rotation matrix.

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ so $B_1 = \sqrt{A} = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}$, $B_2 = \sqrt{-A} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

This method of a matrix factorization can be a subject of **future researches** baised on our criterions of quadraticity.

7 Conclusion

The new linear group which is storage of most of square roots from $SL_2(\mathbb{F}_p)$ is found and investigated by us.

The criterions of the matrix equation $X^2 = A$ solvability over different linear groups with respect to matrix classification by its $tr(A)$ and type of space contracting is found and proved in this paper.

The characterization of form of a square matrix root are closely connected with the solution of matrix factorization that is important, since the factorization of matrices, like polynomials, is related to the factorization of numbers [23], [49], [50], [51].

The method of matrix factorization that we have outlined gives a decomposition of the matrix into two factors of arbitrary shape, not necessarily upper triangular and lower triangular form.

The criterion of roots existing for different classes of matrix — simple and semisimple matrixes from $SL_2(\mathbb{F}_p)$, $SL_2(\mathbb{Z})$ are established.

If a matrix $A \in GL_2(F_p)$ is semisimple with different eigenvalues and at least one an eigenvalue $\lambda_i \in F_{p^2} \setminus F_p$, $i \in \{1, 2\}$, then $\sqrt{A} \in GL_2(F_p)$ iff A satisfies: $(\frac{\lambda_i}{p}) = 1$ in the algebraic extention of degree 2 that is F_{p^2}.

Over method gives answer about existing $\sqrt{M^n}$ without exponenting M to n-th power in contrast with [8], which give answer only after computation $detM^n$ and some real Pell-Lucas numbers by using Bine formula. Out criterion require only the trace of M or only eigenvalues of M.

Acknowledgment

Special thanks to Natalia Vladimirovna Maslova for seminars provided by her and her good questions by the topic. All theoretical results and examples were obtained by Ruslan Skuratovskii. The creation of an article draft was also done by Ruslan Skuratovskii. But the editing of the English text was carried out jointly with the second author — S. Lysenko.

References:

[1] *Micheli, G., Schnyder, R.*, The density of unimodular matrices over integrally closed subrings of function fields, Contemporary Developments in Finite Fields and Applications, World Scientific, (2016). pp. 244-253

[2] *A. Williams, R. V. Skuratovskii,* "Irreducible bases and subgroups of a wreath product in applying to diffeomorphism groups acting on the Mobius band", **2021**. Rendiconti del Circolo Matematico di Palermo Series 2, 70(2), 721-739. https://doi.org/10.1007/s12215-020-00514-5.

[3] *Skuratovskii Ruslan.* "Extended Special Linear group and square root in matrix groups $SL_2(\mathbb{F}_p), SL_2(\mathbb{Z}), ESL_2(\mathbb{F}_p), ESL_2(\mathbb{Z})$ and $GL_2(\mathbb{F}_p)$." arXiv:2307.13873 (2023).

[4] *Jane Gilman.* "Adjoining roots and rational powers of generators in PSL(2, R) and discreteness." [source: arXiv:1705.03539v2 [math.GR] 30 Nov 2017].

[5] *Jane Gilman.* "MEMOIRS of the American Mathematical Society". American Mathematical Society. Providence, Rhode Island. September 1995. Volume 117. Number 561.

[6] *Ihab Ahmad Abd AL-Baset AL-Tamimi*, The Square Roots of 2 2 Invertible Matrices, Advances in Algebra (ISSN 0973-6964) Vol. 3, N0.1(2010), pp 15-18.

[7] *Amit Kulshrestha and Anupam Singh.* "Computing n-th roots in $SL_2(F)$ and Fibonacci polynomials" *Proc. Indian Acad. Sci.* (Math. Sci.) (2020) 130:31 https://doi.org/10.1007/s12044-020-0559-8.

[8] *Saadet Arslan, Fikri Koken.* The Pell and Pell-Lucas Numbers via Square Roots of Matrices. *Journal of Informatics and Mathematical Sciences* Vol. 8, No. 3, pp. 159–166, 2016.

[9] *S. Northshield,* Square roots of 2×2 matrices, Contemporary Mathematics 517 (2010), 289–304.

[10] *Donald Sulivan.* The Square Roots of 2 x 2 Matrices. *University of New Brunswick Fredericton*, N.B., Canada. Mathematics Magazine. pp. 314-317.

[11] *Matej Bresar, Peter Semrl.* The Waring problem for matrix algebras. Israel Journal of Mathematics volume 253, pp. 381–405 (2023).

[12] *Sergiy Maksymenko.* Diffeomorphism groups of Morse-Bott foliation on the solid Klein bottle by Klein bottles parallel to the boundary. Proceedings of the Institute of Mathematics of the National Academy of Sciences of Ukraine (in ukrainian), (2023) vol. 20, No. 1, 896–910.

[13] *Robert Steinberg.* Automorphisms of Finite Linear Groups *https://doi.org/10.4153/CJM-1960-054-6. Published online by Cambridge University Press*

[14] *Ilyas Khan.* Hyperbolic geometry: isometry groups of hyperbolic space. *Inproceedings 2012. https://math.uchicago.edu/ may/REU2012/REUPapers/ Khan.pdf*

[15] *V. A. Roman'kov*. The commutator width of some relatively free lie algebras and nilpotent groups. Siberian Mathematical Journal volume 57, pages 679-695 (2016).

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

[17] *Bandman T., Greuel G.-M., Grunewald F., Kunyavskii B., Pfister G., Plotkin E.* Identities for finite solvable groups and equations in finite simple groups, *Compos. Math.*, 2006, 142(3), 734–764.

[18] *Bandman T., Kunyavskii B.* Criteria for equidistribution of solutions of word equations in $SL(2)$, *J. Algebra*, 2013, 382, 282–302.

[19] *Rosenberger, Gehrard.* All generating pairs of all two-generator Fuchsian groups, Arch. Math. (Basel) 46(1986), no. 3,198-204

[20] *Krishna Kishore, A. Vasiu, Sailun Zhan.* Waring Problem for Matrices over Finite Fields. Journal of Pure and Applied Algebra. 11 June 2023. DOI:10.1016/j.jpaa.2024.107656

[21] *Bovdi V. A., Shchedryk V. P.* Generating solutions of a linear equation and structure of elements of the Zelisko group // Linear Algebra Appl. − 2021. − Volume 625. − P. 55−67.

[22] *Bovdi V., Shchedryk V.* Generating solutions of a linear equation and structure of elements of the Zelisko group II // Quaestiones Mathematicae. – 2022. – 10 pages. – https://doi.org/10.2989/16073606.2022.2112629

[23] *Shchedryk V.* Factorization of matrices over elementary divisor domain // Algebra and Discrete Mathematics. – 2009. – №2. – P. 79–99.

[24] *L. Hua, I. Reiner* Automorphisms of the unimodular group. Trans. Amer. Math. Soc. 71 (1951), 331-348. DOI10.1090S0002-9947-1951-0043847

[25] *Sergiy Maksymenko.* Foliated and leaf preserving diffeomorphisms of simplest Morse-Bott foliations on lens spaces. Submitted on 29 Jan 2023 (v1), *Source: https://arxiv.org/abs/2301.12447v2 last revised 2 Feb 2023 (this version, v2)]*

[26] *Nering, Evar D.*, Linear Algebra and Matrix Theory (2nd ed.), (1970), New York: Wiley, LCCN 76091646.

[27] *Jorg Liesen, Volker Mehrmann.* Linear Algebra. Springer Undergraduate Mathematics Series. Springer International Publishing Switzerland (2015). DOI https://doi.org/10.1007/978-3-319

[28] *N. B. Ladzoryshyn.* Matrix Diophantine equations over quadratic rings and their solutions. Vol. 12 No. 2 (2020). https://doi.org/10.15330/cmp.12.2.368-375

[29] *Yu. I. Merzlyakov,* Automorphisms of two-dimensional congruence groups, *Algebra and Logic,* 10.1007/BF02218574, 12, 4, (262-267), (1973).

[30] *A. R. Chekhlov, P. V. Danchev,* "The strongly invariant extending property for abelian groups", Quaest. Math., 42:8 (2019), 997-1017.

[31] *H. A. Janabi, L. Hethelyi and E. Horvoth* (2020) *Journal of Group Theory.* TI subgroups and depth 3-subgroups in simple Suzuki groups. https://doi.org/10.1515/jgth-2020-0044

[32] *N. D. Zyulyarkina*, "On the commutation graph of cyclic TI-subgroups in linear groups", // Proc. Steklov Inst. Math. (Suppl.), 279, suppl. 1 (2012), 175–181.

[33] *Coxeter, H. S. M. and Moser, W. O. J.* Generators and Relations for Discrete Groups, Issue 14; *Springer Berlin Heidelberg,* 2017, p. 172.

[34] *Tiancheng Zhou,* The Power of Group Generators and Relations: An Examination of the Concept and Its Applications *Journal of Applied Mathematics and Physics* Vol.6 No.11, November 29, 2018 DOI: 10.4236/jamp.2018.611204

[35] *Bray J. N., Holt D. F., Roney-Dougal C.M.* The maximal subgroups of the low-dimensional finite classical groups. *Cambridge: Cambridge Univ. Press*, 2013, 438 p. doi: 10.1017/CBO9781139192576.

[36] *Mark Brittenham and Susan Hermiller* A uniform model for almost convexity and rewriting systems. Journal Journal of Group Theory. Published by De Gruyter March 18, 2015. https://doi.org/10.1515/jgth-2015-0011

[37] *Drozd, Yu. A., R. V. Skuratovskii,* Generators and relations for wreath products. Ukr Math J. (2008), vol. 60. Issue 7, pp. 1168-1171.

[38] *Savelyev N. N.* Lectures on the topology of three-dimensional manifolds. - MCNMO, 2004. (in Russian) - 216 p. — ISBN 5-94057-118-2.

[39] *Saveliev Nikolai.* Lectures on the Topology of 3-Manifolds An Introduction to the Casson Invariant. *University of Miami, Florida, USA. 2nd revised edition* ISBN 9783110250350 2011-12-19, P. 218.

[40] *Martin H. Dull.* Automorphisms of Two-Dimensional Linear Groups over integral domains. *American Journal of Mathematics* Vol. 96, No. 1 (Spring, 1974), pp. 1-40 (40 pages).

[41] *R. M., Guralnick and P.H., Tiep.* Low-dimensional representations of special linear groups in cross characteristics. *Proc. London Math. Soc.* 78 (1999), pp. 116–138.

[42] *A. Putman.* Lectures on the Torelli group. Rice University. 2007. P. 102.

[43] *A. Putman.* Generating the Torelli group October 2011. L'Enseignement Mathématique 58(1) DOI: 10.4171/LEM/58-1-8

[44] *D. Yakymenko.* Sics and the triangle group (3,3,3). Source: [arXiv:2312.13400v1 [quant-ph] 20 Dec 2023].

[45] *D. M. Appleby.* Symmetric informationally complete–positive operator valued measures and the extended Clifford group. *J. Math. Phys.* Volume 46, Issue 5 May 2005. https://doi.org/10.1063/1.1896384

[46] *P. Busch, M. Grabowski, and P. J. Lahti,* Operational Quantum Physics (*Springer,* Berlin, 1995).

[47] *Iatsyshyn, A., Iatsyshyn, A., Kovach, V., Zinovieva, I., Artemchuk, V., Popov, O., Turevych, A.* (2020). Application of open and specialized geoinformation systems for computer modelling studying by students and PhD students. Paper presented at the *CEUR Workshop Proceedings*, 2732 893-908.

[48] *A. Beltran, M. J. Felipe, C. Melchor.* Squares of real conjugacy classes in finite groups. *Annali di Matematica Pura ed Applicata.* Volume 197, pp. 317–328 (2018).

[49] *Koren, Yehuda; Bell, Robert; Volinsky, Chris* (August 2009). "Matrix Factorization Techniques for Recommender Systems". *Computer*. 42 (8): 30–37. CiteSeerX 10.1.1.147.8295. doi:10.1109/MC.2009.263. S2CID 58370896.

[50] *Oleksandr Karelin, Anna Tarasenko.* On Factorization of Functional Operators with Reflection on the Real Axis. *WSEAS TRANSACTIONS on MATHEMATICS* DOI: 10.37394/23206.2021.20.18

[51] *Ruslan V. Skuratovskii.* On commutator subgroups of Sylow 2-subgroups of the alternating group, and the commutator width in wreath products. European Journal of Mathematics (2021), volume 7, pages 353–373.

[52] *Skuratovskii Ruslan.* The Investigation of Euler's Totient Function Preimages for $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$ and the Cardinality of Pretotients in General Case WSEAS Transactions on Mathematics, 2022, 21, pp. 44–52. DOI: 10.37394/23206.2022.21.7.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

All theoretical results and examples were obtained by Ruslan Skuratovskii, the draft of the article was also created by Ruslan Skuratovskii, but the editing of the English text was carried out by him jointly with Lysenko S. O.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.