Journal of Siberian Federal University. Mathematics & Physics 2023, 16(4), 413–419

EDN: BHNJYZ
УДК 512.5

On Generation of the Groups $GL_n(\mathbb{Z})$ and $PGL_n(\mathbb{Z})$ by Three Involutions, Two of which Commute

Irina A. Markovskaya[*]
Yakov N. Nuzhin[†]
Siberian Federal University
Krasnoyarsk, Russian Federation

Received 10.11.2022, received in revised form 24.01.2023, accepted 20.04.2023

Abstract. It is proved that the general linear group $GL_n(\mathbb{Z})$ (its projective image $PGL_n(\mathbb{Z})$ respectively) over the ring of integers $\mathbb{Z}$ is generated by three involutions, two of which commute, if and only if $n \geqslant 5$ (if $n = 2$ and $n \geqslant 5$ respectively).

Keywords: general linear group, ring of integers, generating triples of involutions.

Citation: I.A. Markovskaya, Ya.N. Nuzhin, On Generation of the Groups $GL_n(\mathbb{Z})$ and $PGL_n(\mathbb{Z})$ by Three Involutions, Two of which Commute, J. Sib. Fed. Univ. Math. Phys., 2023, 16(4), 413–419. EDN: BHNJYZ.

Introduction

We call groups, generated by three involutions, two of which commute, $(2\times2,2)$-*generated*.The class of such groups is closed with respect to homomorphic images if, by definition, we consider the identity group as such and we do not exclude the coincidence of two or all three involutions. M. C. Tamburini and P. Zucca [5] have proved that some matrix groups of big enough degree n, depending on the parameter d, over the d-generated commutative are $(2 \times 2, 2)$-generated. Particularly they established $(2 \times 2, 2)$-generation of the special linear group $SL_n(\mathbb{Z})$ over the ring of integers $\mathbb{Z}$ when $n \geqslant 14$. Ya. N. Nuzhin [2] has proved that the projective special linear group $PSL_n(\mathbb{Z})$ over the ring of integers is $(2 \times 2, 2)$-generated if and only if $n \geqslant 5$. Applying methods of the paper [2], we obtain similar criteria for the general linear group $GL_n(\mathbb{Z})$ and its projective image $PGL_n(\mathbb{Z})$.

Theorem 1. *The general linear group $GL_n(\mathbb{Z})$ over the ring of integers $\mathbb{Z}$ is generated by three involutions, two of which commute if and only if $n \geqslant 5$.*

Theorem 2. *The projective general linear group $PGL_n(\mathbb{Z})$ over the ring of integers $\mathbb{Z}$ is generated by three involutions, two of which commute if and only if $n = 2$ and $n \geqslant 5$.*

1. Notations and preliminary results

Further, R is an arbitrary commutative ring with the identity 1, $SL_n(R)$ is a subgroup of matrices with determinant 1 of the general linear group $GL_n(R)$ over the ring R.

[*]mark.i.a@mail.ru
[†]nuzhin2008@rambler.ru

Elementary transvections

$$t_{ij}(k) = E_n + ke_{ij}, \ \ i,j = 1,2,\ldots,n, \ i \neq j, \ k \in R,$$

will be called simply transvections, where E_n is an identity matrix of degree n, and e_{ij} is a $(n \times n)$-matrix with 1 on the position (i,j) and zeros elsewhere. Also let

$$t_{ij}(R) = \langle t_{ij}(k) \mid k \in R \rangle, \ \ i,j = 1,2,\ldots,n, \ i \neq j.$$

For any non-empty subset M of some group, by $\langle M \rangle$ we denote the subgroup generated by the set M. The next lemma is well known (see, for example, [6, p. 107]).

Lemma 1. *The group $SL_n(R)$ over the Euclidean ring R, in particular over any field, is generated by subgroups $t_{ij}(R)$, $i,j = 1,\ldots,n$.*

The ring of integers $\mathbb{Z}$ is Euclidean and $t_{rs}(\mathbb{Z}) = \langle t_{rs}(1) \rangle$, so the corollary of Lemma 1 is

Lemma 2. *The group $SL_n(\mathbb{Z})$ is generated by transvections $t_{ij}(1)$, $i \neq j$, $i, j = 1, 2, \ldots, n$.*

Since the index of the subgroup $SL_n(\mathbb{Z})$ in the group $GL_n(\mathbb{Z})$ is equal to 2, Lemma 2 implies

Lemma 3. *The group $GL_n(\mathbb{Z})$ is generated by transvections $t_{ij}(1)$, $i \neq j$, $i, j = 1, 2, \ldots, n$, and any matrix with determinant -1.*

Set

$$\mu = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

The matrix μ has group order n and the group $\langle \mu \rangle$ acts by conjugations regularly on the set of transvections

$$T = \{t_{1n}(1), t_{i+1i}(1), i = 1,2,\ldots,n-1\},$$

and on the transposed set

$$T' = \{t_{n1}(1), t_{ii+1}(1), i = 1,2,\ldots,n-1\}.$$

By commuting transvections from the set T or from T', all the transvections $t_{ij}(1)$ can be obtained. Therefore, each of the sets T and T' generates the group $SL_n(\mathbb{Z})$. Moreover, by virtue of Lemmas 2 and 3, the following lemma is valid

Lemma 4. *The group $SL_n(\mathbb{Z})$($GL_n(\mathbb{Z})$ respectively) is generated by one of the transvections*

$$t_{1n}(1),\ t_{i+1i}(1),\ t_{n1}(1),\ t_{ii+1}(1), \ \ i = 1,2,\ldots,n-1,$$

and by the matrix $\varepsilon\mu$ for any $(1,-1)$-diagonal matrix ε under condition that $\varepsilon\mu \in SL_n(\mathbb{Z})$ ($det(\varepsilon\mu) = -1$ respectively).

Let I be an ideal of the ring R. Then the natural ring homomorphism $\rho_I:\ R\to R/I$ defines a surjective homomorphism

$$\psi_I:\ M_n(R)\to M_n(R/I)$$

of the ring of $n\times n$-matrices $M_n(R)$ with the usual operations of addition and multiplication, where for any matrix $(a_{ij})\in M_n(R)$ by definition

$$\psi_I:\ (a_{ij})\to(\rho_I(a_{ij})).$$

On the other hand, the homomorphism ρ_I induces a group homomorphism

$$\varphi_I:\ GL_n(R)\to GL_n(R/I),$$

$$\varphi_I:\ SL_n(R)\to SL_n(R/I),$$

where also by definition

$$\varphi_I:\ (a_{ij})\to(\rho_I(a_{ij})).$$

D. A. Suprunenko calls φ_I a *Minkowski homomorphism* [7, p. 95]. However, the homomorphism φ_I is no longer required to be surjective like the homomorphism ψ_I (see [1, Example 1]).

A linear group of type X_n over a finite field of q elements will be denoted by $X_n(q)$

Lemma 5. *The group $PSL_n(2)$ is a homomorphic image of the groups $GL_n(\mathbb{Z})$ and $PGL_n(\mathbb{Z})$.*

Proof. Evidently, $GL_n(2)=PGL_n(2)=SL_n(2)=PSL_n(2)$. Since both groups $GL_n(2)$ and $SL_n(\mathbb{Z})$ are generated by their transvections, and $GL_n(\mathbb{Z})=\langle E_n-2e_{nn}\rangle SL_n(\mathbb{Z})$ and the quotient ring $\mathbb{Z}/I$ by the ideal I generated by the element 2 is isomorphic to a field of two elements, then the homomorphisms $\varphi_I:GL_n(\mathbb{Z})\to GL_n(2)$ and $\varphi_I:PGL_n(\mathbb{Z})\to PGL_n(2)$ are surjective.

The lemma is proved. □

For brevity, the group generated by three involutions, two of which commute, will be called $(2\times2,2)$-*generated*, and, by definition, we consider the identity group as such and do not exclude the coincidence of two or all three involutions. With this definition, the following lemma is valid

Lemma 6. *The class of* $(2\times2,2)$*-generated groups is closed under homomorphic images.*

We use the following notations: $a^b=bab^{-1}$, $[a,b]=aba^{-1}b^{-1}$.

2. Proof of Theorem 1

The case of $\mathbf{n=2}$. The fact that the group $GL_2(\mathbb{Z})$ is not generated by three involutions, two of which commute, was established in [3, Sentence 2.3].

Cases $\mathbf{n=3,4}$. For $n=3,4$ the group $PSL_n(2)$ is not $(2\times2,2)$-generated [4]. Therefore, by virtue of Lemmas 5 and 6, the group $GL_n(\mathbb{Z})$ will also be such. Note that for $n=2$ this argument fails, since the group $PSL_2(2)$ is isomorphic to a dihedral group of order 6, which is $(2\times2,2)$-generated by definition.

Case $\mathbf{n=5}$. Let us show that the group $GL_5(\mathbb{Z})$ is generated by the following three involutions

$$\alpha=\begin{pmatrix}-1&0&0&0&0\\1&1&0&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&-1\end{pmatrix},\quad\beta=\begin{pmatrix}0&0&0&0&-1\\0&0&0&-1&0\\0&0&-1&0&0\\0&-1&0&0&0\\-1&0&0&0&0\end{pmatrix},$$

$$\gamma = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

the first two of which commute. Suppose $M = \langle \alpha, \beta, \gamma \rangle$. Let

$$\eta = \beta\gamma = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

Then

$$\alpha^\eta = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$[\alpha, \alpha^\eta] = t_{31}(-1)t_{41}(1),$$

$$[\alpha, \alpha^\eta]^\eta = t_{42}(-1)t_{52}(1),$$

$$[\alpha, [\alpha, \alpha^\eta]^\eta] = t_{42}(1)t_{51}(-1)t_{52}(-2),$$

$$[\alpha, [\alpha, \alpha^\eta]^\eta]^{\eta^{-1}} = t_{31}(1)t_{41}(-2)t_{45}(-1),$$

$$\left[[\alpha, \alpha^\eta]^\eta, [\alpha, [\alpha, \alpha^\eta]^\eta]^{\eta^{-1}}\right] = t_{42}(1),$$

$$(t_{42}(1))^{\eta^3} = t_{25}(1),$$

$$[t_{42}(1), t_{25}(1)] = t_{45}(1).$$

Thus, M contains the transvection $t_{45}(1)$ and the monomial matrix $\eta = -\mu$ with determinant -1. By Lemma 4 $M = GL_5(\mathbb{Z})$. What was required to show.

Case n = 6. Let us show that the group $GL_6(\mathbb{Z})$ is generated by the following three involutions

$$\alpha = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix},$$

$$\beta = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The involutions β and γ commute. Let us introduce the following notation for some diagonal and monomial matrices by setting

$$d_i = E_n - 2e_{ii},$$
$$d_{ij} = E_n - 2e_{ii} - 2e_{jj},$$
$$n_{ij}^{+} = t_{ij}(1)t_{ji}(-1)t_{ij}(1),$$
$$n_{ij}^{-} = t_{ij}(-1)t_{ji}(1)t_{ij}(-1),$$
$$n_{ij} = d_i n_{ij}^{+}.$$

Obvious relations are valid for the specified elements, which we will use below.

$$(d_i)^2 = (d_{ij})^2 = (n_{ij})^2 = n_{ij}^{+}n_{ij}^{-} = 1,$$
$$(n_{ij}^{+})^2 = (n_{ij}^{-})^2 = d_{ij},$$
$$n_{ij}^{+} = n_{ji}^{-},$$
$$n_{ij} = n_{ji}.$$

Note also that n_{ij} is the permutation matrix corresponding to the transposition (ij). In these notations

$$\alpha = d_{16}t_{21}(1)n_{45},$$
$$\beta = n_{12}n_{34}n_{56},$$
$$\gamma = n_{34}n_{25}n_{16}.$$

Matrix calculations show that

$$\alpha^{\beta} = d_{25}t_{12}(1)n_{36},$$
$$\alpha^{\gamma} = d_{16}t_{56}(1)n_{23},$$
$$\upsilon = (\alpha^{\gamma}\alpha)^2 = t_{21}(1)t_{31}(1)t_{46}(-1)t_{56}(-1),$$
$$\eta = (\alpha\alpha^{\beta})^2 = t_{21}(-1)n_{21}^{-}d_{34}d_{56},$$
$$(\alpha^{\beta})^{\eta} = d_{15}t_{21}(1)n_{36},$$
$$(\alpha(\alpha^{\beta})^{\eta})^2 = d_{34}d_{56},$$
$$(d_{34}d_{56})^{\gamma} = d_{12}d_{34},$$
$$\alpha^{d_{12}d_{34}} = d_{16}d_{45}t_{21}(1)n_{45},$$
$$\alpha\alpha^{d_{12}d_{34}} = d_{45},$$
$$(d_{45})^{\gamma} = d_{23},$$
$$(d_{12}d_{34})d_{45}d_{23} = d_{15},$$
$$d_{15}(\alpha^{\beta})^{\eta} = t_{21}(1)n_{36},$$
$$(t_{21}(1)n_{36})^{\beta} = t_{12}(1)n_{45},$$
$$(d_{15})^{\gamma} = d_{26},$$
$$d_{26}\alpha = d_{12}t_{21}(1)n_{45},$$
$$(d_{12}x_{r_1}(1)n_{45}\eta)^2 = d_{12},$$

$$d_{12}d_{26} = d_{16},$$
$$d_{16}\alpha = t_{21}(1)n_{45},$$
$$(t_{12}(1)n_{45})^{\gamma} = t_{65}(1)n_{23},$$
$$(t_{21}(1)n_{45}t_{65}(1)n_{23})^2 = t_{21}(1)t_{31}(1)t_{64}(1)t_{65}(1),$$
$$\upsilon^{\beta} = t_{12}(1)t_{35}(-1)t_{42}(1)t_{65}(-1),$$
$$(\upsilon^{\beta})^{\eta} = t_{21}(-1)t_{35}(-1)t_{41}(-1)t_{65}(-1),$$
$$[(\upsilon^{\beta})^{\eta}, (t_{21}(1)n_{45}t_{65}(1)n_{23})^2] = t_{61}(1),$$
$$(t_{61}(1))^{\gamma} = t_{16}(1),$$
$$t_{16}(1)t_{61}(-1)t_{16}(1) = n_{61}^{+},$$
$$\beta\gamma = n_{15}n_{26},$$
$$[\alpha, t_{16}(1)] = t_{26}(-1),$$
$$(t_{26}(-1))^{\beta\gamma} = t_{62}(-1),$$
$$t_{26}(1)t_{62}(-1)t_{26}(1) = n_{26}^{+},$$
$$(n_{61}^{+})^{n_{26}^{+}} = n_{21}^{+},$$
$$(n_{21}^{+})^{\gamma} = n_{65}^{-},$$
$$(t_{16}(1))^{n_{26}^{+}} = t_{12}(1),$$
$$d_{16}^{\beta} = d_{25},$$
$$t_{12}(-1)d_{25}\alpha^{\beta} = n_{36},$$
$$n_{36}^{\beta} = n_{45},$$
$$n_{45}^{\gamma} = n_{23},$$
$$(n_{36})^{n_{45}n_{65}^{+}} = n_{34}.$$

Thus, we have obtained monomial elements $n_{21}^{+}, n_{23}, n_{34}, n_{45}, n_{65}^{-}$, which generate a subgroup N containing a representative of each coset of the whole monomial subgroup of $GL_6(\mathbb{Z})$ by its diagonal subgroup. Such a subgroup N acts transitively by conjugations on the subgroups $t_{rs}(\mathbb{Z}) = \langle t_{rs}(1)\rangle$. We have already obtained several transvections $t_{rs}(1)$, and there are also matrices with determinant -1. Thus, by Lemma 3, the involutions α, β, γ generate $GL_6(\mathbb{Z})$.

The case of $\mathbf{n \geqslant 7}$. In the paper [2] for $n \geqslant 7$ in the proof of the generation of the groups $PSL_n(\mathbb{Z})$ for $n = 4k+2$ and $SL_n(\mathbb{Z})$ for $n \neq 4k+2$ by three involutions α, β, γ, the first two of which commute, all calculations, namely, the commutation of two transvections and their conjugation by monomial matrices are carried out up to sign. Therefore, by changing only one of the generating monomial involutions so that its determinant is equal to -1, one can obtain the $(2\times 2, 2)$-generatedness of the group $GL_n(\mathbb{Z})$. The following changes are suitable for our purposes. We replace:

1) β on $\beta' = \sum\limits_{i=1}^{n}(-1)e_{i,n-i+1}$ for $n = 4k+2$ (in this case in [2] the preimage of the involution β in the group $SL_n(\mathbb{Z})$ has order 4);

2) γ on γ', where γ' differs from γ only in the sign of the element at position (n, n) for $n \neq 4k+2$.

The theorem is proved.

Note. There is a typo in [2] on page 70. For $n = 2(2k+1)+1$ (k=7, 11, ...) instead of $\eta_2 = E_n$ there should be $\eta_2 = -E_n$.

3. Proof of Theorem 2

The case of $\mathbf{n = 2}$. The fact that the group $PGL_2(\mathbb{Z})$ is generated by three involutions, two of which commute, was established in [3, Proposition 2.1].

Cases $\mathbf{n = 3, 4}$. For $n = 3, 4$ the group $PSL_n(2)$ is not $(2 \times 2, 2)$-generated [4]. Therefore, by virtue of Lemmas 5 and 6, the group $PGL_n(\mathbb{Z})$ will also be such.

Case $\mathbf{n \geqslant 5}$. The group $PGL_n(\mathbb{Z})$ is a homomorphic image of the group $GL_n(\mathbb{Z})$. Therefore, by virtue of Lemma 6, it follows from Theorem 1 that in this case the group $PGL_n(\mathbb{Z})$ is $(2 \times 2, 2)$-generated.

The theorem is proved.

This work is supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation (Agreement no. 075-02-2023-936).

References

[1] R.I.Gvozdev, Ya.N.Nuzhin, T.B.Shaipova, On generation of groups $SL_n(\mathbb{Z} + i\mathbb{Z})$ and $PSL_n(\mathbb{Z} + i\mathbb{Z})$ by three involutions, two of which commute, *Proceedings of ISU. Series Mathematics,* **40**(2022), 49–62 (in Russian). DOI: 10.26516/1997-7670.2022.40.49

[2] Ya.N.Nuzhin, On generation of the group $PSL_n(Z)$ by three involutions, two of which commute, *Vladikavkaz Math. J.* **10**(2008), no. 1, 68–74 (in Russian).

[3] Ya.N.Nuzhin, I.A.Timofeenko, Generating triplets of involutions of linear groups of dimension 2 over the ring of integers, *Vladikavkaz Math. J.*, **11**(2009), no. 4, 59–62 (in Russian).

[4] Ya.N.Nuzhin, Generating triples of involutions of Chevalley groups over a finite field of characteristic 2, *Algebra and Logic*, **29**(1990), no. 2, 192–206.

[5] M.C.Tamburini, P.Zucca, Generation of Certain Matrix Groups by Three Involutions, Two of Which Commute, *J. of Algebra*, **195**(1997), 650–661.

[6] R.Steinberg, Lectures on Chevalley groups, Moscow, Mir, 1975 (in Russian).

[7] D.A.Suprunenko, Matrix groups, Moscow, Nauka, 1972 (in Russian).

О порождаемости групп $\mathbf{GL_n}(\mathbb{Z})$ и $\mathbf{PGL_n}(\mathbb{Z})$ тремя инволюциями, две из которых перестановочны

Ирина А. Марковская
Яков Н. Нужин
Сибирский федеральный университет
Красноярск, Российская Федерация

Аннотация. Доказано, что общая линейная группа $GL_n(\mathbb{Z})$ (соответственно, ее проективный образ $PGL_n(\mathbb{Z})$) над кольцом целых чисел $\mathbb{Z}$ тогда и только тогда порождается тремя инволюциями, две из которых перестановочны, когда $n \geqslant 5$ (соответственно, когда $n = 2$ и $n \geqslant 5$).

Ключевые слова: общая линейная группа, кольцо целых чисел, порождающие тройки инволюций.