International Journal of Pure and Applied Mathematics
Volume 116 No. 3 2017, 727-737
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v116i3.19

ijpam.eu

ORDER DIMENSIONS OF THE DIAGONAL MATRIX GROUP AND CERTAIN SUBGROUPS OF THE SPECIAL LINEAR GROUP

A. Putmuang[1], J. Sukultanasorn[2], M. Klubmungmee[3], N. Sirasuntorn[4] §
[1,2,3,4]Department of Mathematics
Faculty of Science
Srinakharinwirot University
114 Sukhumvit 23, Wattana District, Bangkok 10110, THAILAND

Abstract: Let G be a group of order m. An *order dimension* of G is the number of different orders of nonidentity elements of G denoted by $\text{odim}(G)$. Let m be a product of prime powers, that is, $m = {p_1}^{m_1}{p_2}^{m_2}\cdots{p_k}^{m_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and m_1 is the greatest of all the powers, i.e. $m_1 \geq m_i$ for all $i \in \{2, 3, \ldots, k\}$. We say that the group G has *property* # if G has a proper subgroup H that $\text{odim}(H) = m_1(m_2+1)\cdots(m_k+1) - 1$.

In this paper, we study order dimensions and the property # of the diagonal matrix group and certain subgroups of the special linear group over a finite field.

AMS Subject Classification: 20H30
Key Words: order dimension, diagonal matrix group, special linear group

1. Introduction

Lagrange's Theorem states that the order of every subgroup of a finite group G divides the order of G. Then possible orders of subgroups of a finite group are counted. Since an order of an element equals an order of the cyclic subgroup generated by that element, we also know the number of all possible orders of elements of a finite group. The alternating group A_4 is a counterexample

Received: June 27, 2017
Revised: September 2, 2017
Published: October 26, 2017

§Correspondence author

of the converse of Lagrange's Theorem. Thus we cannot count the certain number of all orders of elements of each group. In 2008, Ganev [1] studied proper subgroups of a group, and considered the numbers of all possible orders of nonidentity elements of proper subgroups and the maximum value of these numbers. A group that the number of all possible orders of nonidentity elements of a proper subgroup equals the maximum value is said that the group has *the property #*. Moreover, Ganev studied the property # of the group of integers modulo m where m is a positive integer, finitely generated abelian groups, dihedral groups and symmetric groups.

In this paper, we consider the property # of the diagonal matrix group and certain subgroups of the special linear group.

2. Preliminaries and Notations

Ganev [1] defined an *order dimension* of a finite group G that it is the number of different orders of its nonidentity elements, denoted by $\operatorname{odim}(G)$. Then

$$\operatorname{odim}(G) = |\{\circ(a) \,|a \in G \setminus \{e\}\}| \,.$$

Let m be a product of prime powers, that is, $m = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and m_1 is the greatest of all the powers. Denote $b_m = m_1(m_2+1)\cdots(m_k+1)-1$. If a group G of order m has a proper subgroup H with $\operatorname{odim}(H)= b_m$, then we say that group G has *property #*.

Example 2.1 ([1])**.** In $\mathbb{Z}_m$, if $m = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and m_1 is the greatest of all the powers, then $\operatorname{odim}(\langle \bar{p_1} \rangle) = b_m$. Hence $\mathbb{Z}_m$ has property #.

Remark 2.2. Every finite cyclic group has property #.

Ganev also gave the condition for the property # in the following corollary.

Corollary 2.3 ([1])**.** *Let m be a product of primes, $m = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ where p_1 is one of the primes with the highest power, i.e. $m_1 \geq m_i$ for all $i \in \{1, 2, \ldots, k\}$. A group G of order m has property # if and only if G has a subgroup isomorphic to $\mathbb{Z}_{\frac{m}{p_1}}$.*

Let $n \in \mathbb{N}$ and F a finite field. The *general linear group* over F is the group of matrices whose determinant is not zero and the *special linear group* over F is the group of matrices whose determinant is 1. A *diagonal matrix* is a matrix that entries not on the diagonal are all zero. The *diagonal matrix group* or *the group of diagonal invertible matrices* is a subgroup of the general linear group

over F. Then the intersection of the diagonal matrix group and the special linear group over F is an abelian subgroup of the special linear group over F. Besides, the set of all upper triangular $n \times n$ matrices whose determinant is 1 forms a nonabelian subgroup of the special linear group over F if $|F|$ is greater than three. We use the notations for these matrix groups as follows:

$$\begin{aligned} GL(n,F) &= \{\, A \in M_n(F) \,|\, \det(A) \neq 0\}, \\ SL(n,F) &= \{\, A \in GL(n,F) \,|\, \det(A) = 1\}, \\ Diag(n,F) &= \{\, A \in GL(n,F) \,|\, A_{ij} = 0 \text{ when } i \neq j\}, \\ UT(n,F) &= \{\, A \in GL(n,F) \,|\, A_{ij} = 0 \text{ if } i > j\} \end{aligned}$$

where $M_n(F)$ denotes the field of all $n \times n$ matrices over F.

Example 2.4. In $M_4(\mathbb{R})$, let

$$A = \begin{bmatrix} 3 & 0 & 2 & -1 \\ 1 & 2 & 0 & -2 \\ 4 & 0 & 6 & -3 \\ 5 & 0 & 2 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } C = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Then $\det(A) = 20, \det(B) = 1$ and $\det(C) = 0$. Hence $A \in GL(4,\mathbb{R})$, $B \in SL(4,\mathbb{R}) \subseteq GL(4,\mathbb{R})$ but $C \notin GL(4,\mathbb{R})$.

Example 2.5. In $M_4(\mathbb{R})$, let

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 8 \end{bmatrix}, B = \begin{bmatrix} 3 & 1 & 0 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix} \text{ and } C = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 2 & 8 & 0 & 0 \\ 1 & 0 & 6 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Thus $A \in Diag(4,\mathbb{R}) \subseteq UT(4,\mathbb{R})$, $B \in UT(4,\mathbb{R}) \backslash Diag(4,\mathbb{R})$ and $C \notin UT(4,\mathbb{R})$.

We recall the following theorems in abstract algebra which will be used later.

Theorem 2.6 ([2], page 79)**.** *For any group element $a, \circ(a) = |\langle a \rangle|$.*

Theorem 2.7 (*Cauchy's Theorem*)**.** *Let G be a finite group and p be a prime that divides the order of G. Then G has an element of order p.*

Theorem 2.8 ([3], page 265)**.** *If F is a finite field, then $F^* := F \setminus \{0\}$ is a cyclic group.*

3. The Diagonal Matrix Group

From now on, we let F be a finite field and n be a positive integer.

Lemma 3.1. *Let m be a product of prime powers, that is, $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and m_1 is the greatest of all the powers. Then a group G of order m has property # if and only if it has an element with order $\frac{m}{p_1}$.*

Proof. Let m be a product of distinct primes, $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ where m_1 is the greatest of all the powers. Suppose G has property # and $|G| = m$. By Corollary 2.3, there exists a proper subgroup H of G such that $H \cong \mathbb{Z}_{\frac{m}{p_1}}$. By Theorem 2.6, there is $g \in G$ such that $\circ(g) = |\langle g \rangle| = |H| = \frac{m}{p_1}$.

Conversely, Suppose there exists $g \in G$ such that $\circ(g) = \frac{m}{p_1}$. Then $\langle g \rangle \cong \mathbb{Z}_{\frac{m}{p_1}}$. Since $\langle g \rangle$ is a subgroup of G, by Corollary 2.3, G has property #. □

Next, we show examples and theorems for property # of the diagonal matrix group.

Example 3.2. We have $Diag(2,\mathbb{Z}_3) = \left\{ \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix} \right\}$. Then $|Diag(2,\mathbb{Z}_3)| = 4 = 2^2$. Since $\circ\left(\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix} \right) = 2 = \frac{4}{2}$, by Lemma 3.1, $Diag(2,\mathbb{Z}_3)$ has property #.

Example 3.3. Consider orders of all nonidentity elements of $Diag(2,\mathbb{Z}_5)$. Then $\operatorname{odim}(Diag(2,\mathbb{Z}_5)) = 2$. Let H be a proper subgroup of $Diag(2,\mathbb{Z}_5)$. Thus $\operatorname{odim}(H) \leq \operatorname{odim}(Diag(2,\mathbb{Z}_5)) = 2$. But $b_{16} = 3$, $\operatorname{odim}(H) \neq b_{16}$. This implies that $Diag(2,\mathbb{Z}_5)$ does not have property #.

Theorem 3.4. *If $|F^*|$ is a prime, then $Diag(2, F)$ has property #.*

Proof. Assume $|F^*| = p$ where p is a prime. We have

$$Diag(2, F) = \left\{ \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \middle| \, a_1, a_2 \in F^* \right\}.$$

Then $m = |Diag(2, F)| = p^2$, and hence $\frac{m}{p} = \frac{p^2}{p} = p$. Since $p \,\Big|\, |Diag(2, F)|$, by Cauchy's Theorem, there exists an element $\begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$ of $Diag(2, F)$ such

that $\circ\left(\begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}\right) = p = \frac{m}{p}$. By Lemma 3.1, $Diag(2, F)$ has property #. □

Theorem 3.5. *If $|F^*|$ is a prime and $n > 2$, then $Diag(n, F)$ has no property #.*

Proof. Assume $|F^*| = p$ where p is a prime and $n > 2$. Then $m = |Diag(n, F)| = p^n$, so $\frac{m}{p} = \frac{p^n}{p} = p^{n-1}$. Let $A \in Diag(n, F)$. Then

$$A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n \end{bmatrix} \text{ for some } a_1, a_2, \ldots, a_n \in F^*,$$

so $\circ(A) = \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n))$. We have $|F^*| = p$. Then $\text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) = p^l$ where $l \in \{0, 1\}$. It follows that

$$\begin{aligned} \circ(A) &= \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) \\ &< p^{n-1} = \frac{m}{p}. \end{aligned}$$

By Lemma 3.1, $Diag(n, F)$ has no property #. □

Theorem 3.6. *If $|F^*|$ is not a prime, then $Diag(n, F)$ has no property # for all $n \geq 2$.*

Proof. Assume $|F^*|$ is not a prime.

Case 1: $|F^*| = p_1^{m_1}$ for some prime p_1 and $m_1 > 1$.

Then $m = |Diag(n, F)| = (|F^*|)^n = p_1^{nm_1}$ and $\frac{m}{p_1} = p_1^{nm_1 - 1}$. Let $A \in Diag(n, F)$. Then

$$A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n \end{bmatrix} \text{ for some } a_1, a_2, \ldots, a_n \in F^*,$$

so $\circ(A) = \text{lcm}(\circ(a_1), \circ(a_2), \cdots, \circ(a_n))$. Since for all $i \in \{1, 2, \ldots, n\}$, $a_i \in F^*$ and $\circ(a_i) = p_1^{l_i}$ where $0 \leq l_i \leq m_1$, $\text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) = p_1^u$ where $u = \max\{l_1, l_2, \ldots, l_n\}$. Thus $u \leq m_1$, so $p_1^u \leq p_1^{m_1}$. Since $m_1 + 1 < m_1 + m_1 \leq nm_1$, it follows that $\circ(A) = p_1^u \leq p_1^{m_1} < p_1^{nm_1 - 1} = \frac{m}{p_1}$.

Case 2: $|F^*| = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ for some distinct primes $p_1, p_2, \ldots, p_k$, $k \geq 2$ and $m_1, m_2, \ldots, m_k \in \mathbb{N}$ such that $m_1 \geq m_j$ for all j.

Then $m = |Diag(n, F)| = (|F^*|)^n = (p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k})^n = p_1^{nm_1}p_2^{nm_2}\cdots p_k^{nm_k}$ and $\frac{m}{p_1} = p_1^{nm_1-1}p_2^{nm_2}\cdots p_k^{nm_k}$. Let $A \in Diag(n, F)$. Then

$$A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n \end{bmatrix} \text{ for some } a_1, a_2, \ldots, a_n \in F^*.$$

Thus for all $i \in \{1, 2, \ldots, n\}, a_i \in F^*$ and $\circ(a_i) = p_1^{l_{i1}}p_2^{l_{i2}}\cdots p_k^{l_{ik}}$ where $l_{ij} \leq m_j$ for all $j \in \{1, 2, \ldots, k\}$. It follows that $\circ(A) = \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) = p_1^{u_1}p_2^{u_2}\cdots p_k^{u_k}$ where $u_j =$
$\max\{l_{1j}, l_{2j}, \ldots, l_{nj}\}$ and $u_j \leq m_j < nm_j$ for all $j \in \{1, 2, \ldots, k\}$. We have $m_1 \leq nm_1 - 1$. Then

$$\begin{aligned} \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) &= p_1^{u_1}p_2^{u_2}\cdots p_k^{u_k} \\ &\leq p_1^{m_1}p_2^{u_2}\cdots p_k^{u_k} \\ &\leq p_1^{nm_1-1}p_2^{u_2}\cdots p_k^{u_k} \\ &< p_1^{nm_1-1}p_2^{nm_2}\cdots p_k^{nm_k} = \frac{m}{p_1}. \end{aligned}$$

Thus $\circ(A) = \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) < \frac{m}{p_1}$. This proves that all elements of $Diag(n, F)$ have orders not equal to $\frac{m}{p_1}$ implying that $Diag(n, F)$ has no property #. □

Corollary 3.7. *$Diag(n, F)$ has property # if and only if $|F^*|$ is a prime and $n = 2$.*

Proof. It is obtained from Theorem 3.4 - Theorem 3.6 □

4. Subgroups of the Special Linear Group

Next, we study the property # of two subgroups of the special linear group over F. The first subgroup is the intersection of the diagonal matrix group and the special linear group over F denoted by $Diag(n, F) \cap SL(n, F)$. The results of this subgroup are shown in Theorem 4.1 - Theorem 4.5. The second subgroup is the group of all upper triangular $n \times n$ matrices whose determinant is 1, which will be shown later.

Theorem 4.1. *$Diag(2,F)\cap SL(2,F)$ has property #.*

Proof. We have

$$Diag(2,F)\cap SL(2,F)=\left\{\begin{bmatrix}a&0\\0&b\end{bmatrix}\middle|\, a,b\in F^{*}\text{and } ab=1\right\}$$
$$=\left\{\begin{bmatrix}a&0\\0&a^{-1}\end{bmatrix}\middle|\, a\in F^{*}\right\}.$$

Then $Diag(2,F)\cap SL(2,F)\cong F^{*}$ with an isomorphism from F^{*} into $Diag(2,F)\cap SL(2,F)$ defined by $\phi(a)=\begin{bmatrix}a&0\\0&a^{-1}\end{bmatrix}$ for all $a\in F^{*}$. By Theorem 2.8, $Diag(2,F)\cap SL(2,F)$ is a cyclic group. By Remark 2.2, $Diag(2,F)\cap SL(2,F)$ has property #. □

Theorem 4.2. *$|Diag(n,F)\cap SL(n,F)|=|F^{*}|^{n-1}$ for all $n\in\mathbb{N}$.*

Proof. For each $a\in F^{*}$ and $n\in\mathbb{N}$, let

$$D_a^n=\{(a_1,a_2,\ldots,a_n)\in(F^{*})^n|a_1a_2\cdots a_n=a\}.$$

First, we will show that $|D_a^n|=|F^{*}|^{n-1}$ for all $a\in F^{*}$ and $n\in\mathbb{N}$ by the mathematical induction on n. Let $a\in F^{*}$. Then $D_a^1=\{(a_1)\in(F^{*})^1|a_1=a\}=\{(a)\}$, so $\left|D_a^1\right|=1=|F^{*}|^{1-1}$. Next, assume that for all $a\in F^{*}$, $\left|D_a^k\right|=|F^{*}|^{k-1}$ where $k\in\mathbb{N}$. Let $a\in F^{*}$. Then

$$D_a^{k+1}=\{(a_1,a_2,\ldots,a_{k+1})\in(F^{*})^{k+1}|a_1a_2\cdots a_{k+1}=a\}$$
$$=\{(b,a_1,\ldots,a_k)\in(F^{*})^{k+1}|ba_1\cdots a_k=a\}.$$

Fix $b\in F^{*}$. We have $D_{b^{-1}a}^k=\{(a_1,a_2,\ldots,a_k)\in(F^{*})^k|a_1a_2\cdots a_k=b^{-1}a\}$. Since $b^{-1}a\in F^{*}$, $\left|D_{b^{-1}a}^k\right|=|F^{*}|^{k-1}$, by assumption. Thus $\left|D_a^{k+1}\right|=|F^{*}|\cdot|F^{*}|^{k-1}=|F^{*}|^{(k+1)-1}$. By the mathematical induction, $|D_a^n|=|F^{*}|^{n-1}$ for all $a\in F^{*}$ and $n\in\mathbb{N}$. Since for all $n\in\mathbb{N}$,

$$Diag(n,F)\cap SL(n,F)=\left\{\begin{bmatrix}a_1&0&\cdots&0\\0&a_2&\cdots&\vdots\\\vdots&\vdots&\ddots&\vdots\\0&\cdots&\cdots&a_n\end{bmatrix}\middle|\, a_1a_2\cdots a_n=1\right\}$$

and $D_1^n=\{(a_1,a_2,\ldots,a_n)\in(F^{*})^n|a_1a_2\cdots a_n=1\}$, it follows that

$$|Diag(n,F)\cap SL(n,F)|=|D_1^n|=|F^{*}|^{n-1}.$$

□

Theorem 4.3. *If $|F^*|$ is a prime, then $Diag(3,F)\cap SL(3,F)$ has property #.*

Proof. Assume $|F^*| = p$ for some prime p. We have

$$Diag(3,F)\cap SL(3,F) = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} \middle| \, a,b,c \in F^* \text{ and } abc = 1 \right\}.$$

Fix $a \in |F^*|$ and let $A_a = \left\{ (b,c) \middle| \, b,c \in F^* \text{and } bc = a^{-1} \right\}$. Since $(F^*,\cdot)$ is a group, $|A_a| = |F^*|$. It follows that $m = |Diag(3,F)\cap SL(3,F)| = |F^*|\cdot|F^*| = (|F^*|)^2 = p^2$, so $\frac{m}{p} = \frac{p^2}{p} = p$. By Cauchy's Theorem, there is a matrix A of $Diag(3,F)\cap SL(3,F)$ such that $\circ(A) = p = \frac{m}{p}$. By Lemma 3.1, $Diag(3,F)\cap SL(3,F)$ has property #. □

Theorem 4.4. *If $|F^*|$ is not a prime, then $Diag(3,F)\cap SL(3,F)$ has no property #.*

Proof. Assume $|F^*|$ is not a prime.

Case 1: $|F^*| = p_1^{m_1}$ for some prime p_1 and $m_1 > 1$.

Then $m = |Diag(3,F)\cap SL(3,F)| = p_1^{2m_1}$, so $\frac{m}{p_1} = \frac{p_1^{2m_1}}{p_1} = p_1^{2m_1-1}$. Let $a,b,c \in F^*$. Then $\circ(a) = p_1^{l_1}$, $\circ(b) = p_1^{l_2}$, $\circ(c) = p_1^{l_3}$ where $0 \le l_1,\ l_2,\ l_3 \le m_1$. Let $u = \max\{l_1,l_2,l_3\}$. Thus $\circ \left(\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} \right) = \text{lcm}(\circ(a),\circ(b),\circ(c)) = p_1^u \le p_1^{m_1} < p_1^{m_1+(m_1-1)} < p_1^{2m_1-1} = \frac{m}{p_1}$.

Case 2: $|F^*| = p_1^{m_1}p_2^{m_1}\cdots p_k^{m_k}$ for some distinct primes $p_1,p_2,\ldots p_k$, $k \ge 2$ and $m_1,m_2,\ldots,m_k \in \mathbb{N}$ such that $m_1 \ge m_j$ for all j.

Then $m = |Diag(3,F)\cap SL(3,F)| = p_1^{2m_1}p_2^{2m_1}\cdots p_k^{2m_k}$, so

$$\frac{m}{p_1} = p_1^{2m_1-1}p_2^{2m_1}\cdots p_k^{2m_k}.$$

Let $a_1,a_2,a_3 \in F^*$ and $\circ(a_i) = p_1^{l_{i1}}p_2^{l_{i2}}\cdots p_k^{l_{ik}}$ for all $l_{ij} \le m_j$, $i \in \{1,2,3\}$ and $j \in \{1,2,\ldots,k\}$. It follows that

$$\circ \left(\begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{bmatrix} \right) = \text{lcm}(\circ(a_1),\circ(a_2),\circ(a_3))$$

$$\begin{aligned} &= p_1^{u_1} p_1^{u_2} \cdots p_k^{u_k} \\ &\leq p_1^{2m_1-1} p_2^{u_2} \cdots p_k^{u_k} \\ &< p_1^{2m_1-1} p_2^{2m_1} \cdots p_k^{2m_k} = \frac{m}{p_1}. \end{aligned}$$

where $u_j = \max\{l_{1j}, l_{2j}, l_{3j}\}$. This means that no element of $Diag(3,F) \cap SL(3,F)$ has order $\frac{m}{p_1}$. By Lemma 3.1, $Diag(3,F) \cap SL(3,F)$ has no property #. □

Theorem 4.5. *Diag(n, F)∩ SL(n, F) has no property # if n > 4.*

Proof. Assume $n > 4$. By Theorem 4.2, $m = |Diag(n,F) \cap SL(n,F)| = (|F^*|)^{n-1}$.

Case 1: $|F^*| = p_1^{m_1}$ for some prime p_1 and $m_1 > 1$.

Then $\frac{m}{p_1} = \frac{(p_1^{m_1})^{n-1}}{p_1} = p_1^{(n-1)m_1-1}$. Let $A \in Diag(n,F) \cap SL(n,F)$. Thus

$$A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n \end{bmatrix} \text{ for some } a_1, a_2, \ldots, a_n \in F^*,$$

so $\circ(A) = \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n))$. Since $a_i \in F^*$, we have that $\circ(a_i) = p_1^{l_i}$ where $0 \leq l_i \leq m_1$ and $i \in \{1, 2, \ldots, n\}$. Hence $\text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) = p_1^{u_1}$ where $u_1 = \max\{l_1, l_2, \ldots, l_n\}$. Thus $\circ(A) = p_1^{u_1} \leq p_1^{m_1} < p_1^{m_1+(n-2)m_1-1} = p_1^{(n-1)m_1-1} = \frac{m}{p_1}$.

Case 2: $|F^*| = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ for some distinct primes $p_1, p_2, \ldots p_k$, $k \geq 2$ and $m_1, m_2, \ldots, m_k \in \mathbb{N}$ such that $m_1 \geq m_j$ for all j.

Then $\frac{m}{p_1} = p_1^{(n-1)m_1} p_2^{(n-1)m_2} \cdots p_k^{(n-1)m_k}$. Let $A \in Diag(n,F) \cap SL(n,F)$. Then $A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n \end{bmatrix}$ for some $a_1, a_2, \ldots, a_n \in F^*$. Since $|F^*| = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, $\circ(a_i) = p_1^{l_{i1}} p_2^{l_{i2}} \cdots p_k^{l_{ik}}$ for all $l_{ij} \leq m_j, i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, k\}$. Thus

$$\begin{aligned} \circ(A) &= \text{lcm}(\circ(a_1), \circ(a_2), \ldots, \circ(a_n)) \\ &= p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k} \end{aligned}$$

$$\begin{aligned} &\leq p_1^{(n-1)m_1-1} p_2^{u_2} \cdots p_k^{u_k} \\ &< p_1^{(n-1)m_1-1} p_2^{(n-1)m_2} \cdots p_k^{(n-1)m_k} = \frac{m}{p_1} \end{aligned}$$

where $u_j = \max\{l_{1j}, l_{2j}, \ldots, l_{nj}\}$. By Lemma 3.1, $Diag(3,F) \cap SL(3,F)$ has no property #. □

Lastly, we give some examples and the theorem for property # of the group of all upper triangular 2×2 matrices whose determinant is 1 denoted by $UT(2,\mathbb{Z}_p) \cap SL(2,\mathbb{Z}_p)$.

Example 4.6. Consider $UT(2,\mathbb{Z}_3) \cap SL(2,\mathbb{Z}_3) = \left\{ \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} \begin{bmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{1} \\ \bar{0} & \bar{2} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{2} \\ \bar{0} & \bar{2} \end{bmatrix} \right\}$. Then $m = |UT(2,\mathbb{Z}_3) \cap SL(2,\mathbb{Z}_3)| = 6 = 2 \times 3$ and $\frac{m}{p_1} = \frac{6}{2} = 3$ or $\frac{m}{p_1} = \frac{6}{3} = 2$. We have $\circ \left(\begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} \right) = 3$ and $\circ \left(\begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix} \right) = 2$. By Lemma 3.1, $UT(2,\mathbb{Z}_3) \cap SL(2,\mathbb{Z}_3)$ has property #.

Example 4.7. Consider $UT(2,\mathbb{Z}_5) \cap SL(2,\mathbb{Z}_5)$. We have

$$m = |UT(2,\mathbb{Z}_5) \cap SL(2,\mathbb{Z}_5)| = 2^2 \times 5,$$

so $\frac{m}{p_1} = 10$. Since $\circ \left(\begin{bmatrix} \bar{4} & \bar{1} \\ \bar{0} & \bar{4} \end{bmatrix} \right) = 10$, by Lemma 3.1, $UT(2,\mathbb{Z}_5) \cap SL(2,\mathbb{Z}_5)$ has property #. Note that $UT(2,\mathbb{Z}_5) \cap SL(2,\mathbb{Z}_5)$ is a nonabelian group.

Theorem 4.8. *For any prime p, $UT(2,\mathbb{Z}_p) \cap SL(2,\mathbb{Z}_p)$ has property #.*

Proof. Let $\left|\mathbb{Z}_p^*\right| = p - 1 = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k}$ for some distinct primes

$$q_1, q_2, \ldots, q_k, k \geq 2$$

and $m_1, m_2, \ldots, m_k \in \mathbb{N}$ and $m_1 \geq m_j$ for all $j \in \{1, 2, \ldots, k\}$. Since $UT(2,\mathbb{Z}_p) \cap SL(2,\mathbb{Z}_p) = \left\{ \begin{bmatrix} a & b \\ \bar{0} & a^{-1} \end{bmatrix} \middle| a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p \right\}$, $m = |UT(2,\mathbb{Z}_p) \cap SL(2,\mathbb{Z}_p)| = (p-1)p = (q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k})p$. Then $\frac{m}{q_1} = (q_1^{m_1-1} q_2^{m_2} \cdots q_k^{m_k})p$.

Firstly, we will show that $\circ \left(\begin{bmatrix} \bar{1} & c \\ \bar{0} & \bar{1} \end{bmatrix} \right) = p$ for all $c \in \mathbb{Z}_p^*$. Let $c \in \mathbb{Z}_p^*$. Since p is the least positive integer such that $pc = \underbrace{c + c + \cdots + c}_{p \text{ terms}} = 0$, p is the least positive integer such that $\begin{bmatrix} \bar{1} & c \\ \bar{0} & \bar{1} \end{bmatrix}^p = \begin{bmatrix} \bar{1} & pc \\ \bar{0} & \bar{1} \end{bmatrix} = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}$. This implies that

$\circ\left(\begin{bmatrix}\bar{1} & c\\ \bar{0} & \bar{1}\end{bmatrix}\right) = p.$

Next, let $a \in \mathbb{Z}_p^*$ and $b \in \mathbb{Z}_p$. Consider $\circ(a)$ in $(\mathbb{Z}_p^*, \cdot)$. Since $\left(\begin{bmatrix}a & b\\ \bar{0} & a^{-1}\end{bmatrix}\right)^{\circ(a)}$ $= \begin{bmatrix}a^{\circ(a)} & b\\ \bar{0} & (a^{-1})^{\circ(a)}\end{bmatrix} = \begin{bmatrix}\bar{1} & c\\ \bar{0} & \bar{1}\end{bmatrix}$ for some $c \in \mathbb{Z}_p$, it follows that $\circ\left(\begin{bmatrix}a & b\\ \bar{0} & a^{-1}\end{bmatrix}\right)$ is a multiple of $\circ(a)$. Then $\circ\left(\begin{bmatrix}a & b\\ \bar{0} & a^{-1}\end{bmatrix}\right) = \circ(a)s$ for some $s \in \mathbb{N}$. If $c = 0$, then $s = 1$ and $\circ\left(\begin{bmatrix}a & b\\ \bar{0} & a^{-1}\end{bmatrix}\right) = \circ(a)$. Suppose $c \neq 0$. Since $\circ\left(\begin{bmatrix}\bar{1} & c\\ \bar{0} & \bar{1}\end{bmatrix}\right) = p$, $\left(\begin{bmatrix}a & b\\ \bar{0} & a^{-1}\end{bmatrix}^{\circ(a)}\right)^p = \begin{bmatrix}\bar{1} & c\\ \bar{0} & \bar{1}\end{bmatrix}^p = \begin{bmatrix}\bar{1} & \bar{0}\\ \bar{0} & \bar{1}\end{bmatrix}$. This proves that $\circ\left(\begin{bmatrix}a & b\\ \bar{0} & a^{-1}\end{bmatrix}\right) = \circ(a)$ or $\circ(a)p$.

Lastly, we will show the element of $UT(2, \mathbb{Z}_p) \cap SL(2, \mathbb{Z}_p)$ with order $\frac{m}{q_1}$. By Theorem 2.8, $\mathbb{Z}_p^*$ is a cyclic group. Since $\left|\mathbb{Z}_p^*\right| = p-1 = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k}$, there exists $d \in \mathbb{Z}_p^*$ such that $\circ(d) = q_1^{m_1-1} q_2^{m_2} \cdots q_k^{m_k}$. It follows that $\begin{bmatrix}d & \bar{1}\\ \bar{0} & d^{-1}\end{bmatrix} \in$ $UT(2, \mathbb{Z}_p) \cap SL(2, \mathbb{Z}_p)$ such that $\circ\left(\begin{bmatrix}d & \bar{1}\\ \bar{0} & d^{-1}\end{bmatrix}\right) = \circ(d)p = (q_1^{m_1-1} q_2^{m_2} \cdots q_k^{m_k})p$ $= \frac{m}{q_1}$. By Lemma 3.1, $UT(2, \mathbb{Z}_p) \cap SL(2, \mathbb{Z}_p)$ has property #. □

References

[1] I. Ganev, Order Dimension of Subgroups, *Rose-Hulman Undergraduate Mathematics Journal*, **9**, No. 2 (2008), 1-10.

[2] J. A. Gallian, *Contemporary Abstract Algebra* (*Eighth Edition*), Cengage Learning, USA (2013).

[3] N. I. Herstein, *Abstract Algebra* (*Second Edition*), Collier Macmillan Publishers, England (1990).