<table>
<thead>
<tr>
<th>Title</th>
<th>On symmetric sets of unimodular symmetric matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Nobusawa, Nobuo; Ikeda, Yasuhiko</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 14(3) P.471–P.480</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1977</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/11362">https://doi.org/10.18910/11362</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/11362</td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
</tbody>
</table>
ON SYMMETRIC SETS OF UNIMODULAR SYMMETRIC MATRICES

YASUHIKO IKEDA AND NOBUO NOBUSAWA

(Received June 17, 1976)

1. Introduction

A binary system $A$ is called a symmetric set if (1) $a\circ a = a$, (2) $(a\circ b)\circ b = a$ and (3) $(a\circ b)\circ c = (a\circ c)\circ (b\circ c)$ for elements $a$, $b$ and $c$ in $A$. Define a mapping $S_a$ of $A$ for an element $a$ in $A$ by $S_a(x) = x\circ a$. As in [2], [3] and [4], we denote $S_a(x)$ by $xS_a$. $S_a$ is a homomorphism of $A$ due to (3), and is an automorphism of $A$ due to (2). Every group is a symmetric set by a definition: $a\circ b = ba^{-1}b$. A subset of a group which is closed under this operation is also a symmetric set.

In this paper, we consider a symmetric set which is a subset of the group $SL_n(K)$ consisting of all unimodular symmetric matrices. We denote it by $SM_n(K)$. For a symmetric set $A$, we consider a subgroup of the group of automorphisms of $A$ generated by all $S_aS_b$ ($a$ and $b$ in $A$), and call it the group of displacements of $A$. We can show that the group of displacements of $SM_n(K)$ is isomorphic to $SL_n(K)/\{\pm 1\}$ if $n \geq 3$ or $n \geq 2$ when $K = F_q$ (Theorem 5). Also we can show that $PSM_n(K)$, which is defined in a similar way that $PSL_n(K)$ is defined, has its group of displacements isomorphic to $PSL_n(K)$ under the above condition (Theorem 6). A symmetric set $A$ is called transitive if $A = aH$, where $a$ is an element of $A$ and $H$ is the group of displacements. A subset $B$ of $A$ is called an ideal if $BS_a \subseteq B$ for every element $a$ in $A$. For an element $a$ in $A$, $aH$ is an ideal since $aHS_a = aS_aH = aS_aS_aH = aH$ for every element $x$ in $A$. Therefore, $A$ is transitive if and only if $A$ has no ideal other than itself. Let $F_q$ be a finite field of $q$ elements ($q = p^n$). We can show that $SM_n(F_q)$ is transitive if $p = 2$ or if $n$ is odd, and that $SM_n(F_q)$ consists of two disjoint ideals both of which are transitive if $n$ is even and $p = 2$ (Theorem 7).

A symmetric subset $B$ of $A$ is called quasi-normal if $BT \cap B = B$ or $\phi$ for every element $T$ of the group of displacements. When $A$ has no proper quasi-normal symmetric subset, we say that $A$ is simple. In [4], it was shown that if $A$ is simple (in this case, $A$ is transitive as noted above) then the group of displacements is either a simple group or a direct product of two isomorphic simple groups. In [4], we show some examples of $PSM_n(F_q)$. The first example is $PSM_3(F_2)$, which is shown to be a simple symmetric set of 28 elements.
The second example is PSM$(F_7)$, which we show consists of 21 elements and is not simple. We analyze the structure of it and show that PSL$(F_7)$ (which is isomorphic to PSL$_3(F_2)$ and is simple) is a subgroup of $A_7$. The third example is one of ideals of PSM$(F_7)$ which consists of unimodular symmetric matrices with zero diagonal. It has 28 elements and we can show that it is isomorphic to a symmetric set of all transpositions in $S_8$. This reestablishes the well known theorem that PSL$_3(F_2)$ is isomorphic to $A_8$.

2. Unimodular symmetric matrices

Theorem 1. SL$_n(K)$ is generated by unimodular symmetric matrices if $n \geq 3$ or $n \geq 2$ when $K = F_3$.

Proof. Consider a subgroup of SL$_n(K)$ generated by all unimodular symmetric matrices. It is a normal subgroup because if $s$ is a symmetric matrix and $u$ is a non singular matrix then $u^{-1}su = (u'u)^{-1}(u'su)$ which is a product of symmetric matrices. The subgroup clearly contains the center of SL$_n(K)$ properly so that it must coincide with SL$_n(K)$ if $n \geq 3$ or $n \geq 2$ when $K = F_2$ or $F_3$, since PSL$_n(K)$ is simple. If $n = 2$ and $K = F_2$, Theorem 1 follows directly from $r_1 = r_0 r_\eta$ and $r_1 \mu r_\eta r_0$. If $n = 2$ and $K = F_3$, Theorem 1 does not hold since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is not expressed as a product of unimodular symmetric matrices.

Two matrices $a$ and $b$ are said to be congruent if $b = uau$ with a non singular matrix $u$. Suppose that $a$ is congruent to $1$ (the identity matrix) and that $\det a = 1$. Then $1 = u'au$, where we may assume that $\det u = 1$, because otherwise $\det u = -1$ and then we can replace $u$ by $uv$ with $v = \begin{bmatrix} -1 & 0 \\ 1 & \cdots \\ 0 & 1 \end{bmatrix}$.

Theorem 2. Suppose that $n \geq 2$ and $p \neq 2$. Then every unimodular symmetric matrix in SL$_n(F_q)$ is congruent to $1$.

Theorem 2 is known. ([1], p. 16)

Theorem 3. Suppose that $n \geq 2$ and $q = 2^m$. If $n$ is odd, every unimodular symmetric matrix in SL$_n(F_q)$ is congruent to $1$. If $n$ is even, every unimodular symmetric matrix in SL$_n(F_q)$ is congruent either to $1$ or to $J \oplus J \oplus \cdots \oplus J$, where $J = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. The latter occurs if and only if every diagonal entry of the symmetric matrix is zero.

Proof. First, we show a lemma.
Lemma. Suppose that the characteristic of \( K \) is 2. If every diagonal entry of a symmetric matrix \( s \) over \( K \) is zero, then \( u'su \) has the same property where \( u \) is any matrix over \( K \).

Proof. Let \( s=(a_{ij}) \), \( u=(b_{ij}) \), and \( w=(c_{ij}) \). Then \( \Lambda, \cdot, \cdot =\#, \cdot, \cdot \) and \( c_{ii} = \sum_{k,j} b_{ik} a_{kj} b_{ji} = \sum_{k,j} b_{ik} (a_{kj} + a_{jk}) b_{ji} = 0 \) since \( a_{kj} + a_{jk} = 2a_{kj} = 0 \).

Now we return to the proof of Theorem 3. Let \( s=(a_{ij}) \) be a symmetric matrix in \( SL_n(F_q) \). Suppose that \( a_{ii}=0 \) for all \( i \). Then \( a_{1k} \neq 0 \) for some \( k \). Taking a product of elementary matrices for \( u \), we have that, in \( u'su=(b_{ij}) \), \( b_{1k} \neq 0 \) and \( b_{ij}=0 \) for all \( j \neq 2 \). Since \( b_{ij}=b_{ij} = 0 \), we can apply the same argument to the second row (and hence to the second column at the same time) to get a matrix \( (c_{ij}) \) congruent to \( s \) such that \( (c_{ij})=\begin{bmatrix} 0 & c \\ c & 0 \end{bmatrix} \oplus s' \), where \( s' \) is a symmetric matrix of \( (n-2) \times (n-2) \). Then take an element \( d \) in \( F_q \) such that \( d^2 = c^{-1} \), and let \( u=\begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix} \oplus I_{n-2} \), where \( I_{n-2} \) is the identity matrix of \( (n-2) \times (n-2) \). Thusfar, we have seen that \( s \) is congruent to \( J \oplus s' \). By Lemma, \( s' \) has the zero diagonal. Proceeding inductively, we can get \( J \oplus J \oplus \cdots \oplus J \) which is congruent to \( s \), if \( s \) has the zero diagonal. In this case, \( n \) must be even. Next, suppose that \( a_{i1} \neq 0 \) for some \( i \). As in above, we can find \( u \) such that \( u'su=\begin{bmatrix} 1 \\ \oplus s' \end{bmatrix} \), where \( s' \) is of \( (n-1) \times (n-1) \). By induction, \( s' \) is congruent either to \( I_{n-1} \) or to \( J \oplus J \oplus \cdots \oplus J \). In the former case, \( s \) is congruent to \( 1=I \). In the latter case, we just observe that

\[
[1] \oplus J = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.
\]

So, we can reduce \( s \) to the identity matrix by congruence.

Theorem 4. Suppose that \( n \) is even and \( q=2^n \). Then \( SL_n(F_q) \) is generated by \( a^{-1}b \) where \( a \) and \( b \) are unimodular symmetric matrices with zero diagonal. Also, \( SL_n(F_q) \) is generated by \( c^{-1}d \) where \( c \) and \( d \) are unimodular symmetric matrices which have at least one non zero entry in diagonal.

Proof. For \( a \) and \( b \) in Theorem 4, we have \( s^{-1}(a^{-1}b)s=(sas)^{-1}(sbs) \), where \( s \) is a symmetric matrix in \( SL_n(F_q) \). By Lemma, \( sas \) and \( sbs \) have zero diagonal. Since \( SL_n(F_q) \) is generated by symmetric matrices by Theorem 1, the above fact implies that the subgroup of \( SL_n(F_q) \) generated by all \( a^{-1}b \) is a normal subgroup. On the other hand, the center of \( SL_n(F_q) \) consists of \( zI \) where \( z \) is an element of \( F_q \) such that \( z^n=1 \). Since \( zI=a^{-1}(za) \), the center of \( SL_n(F_q) \) is contained in the subgroup generated by \( a^{-1}b \). It is also easy to see that the subgroup contains an element which is not contained in the center. Again, by the simplicity of \( PSL_n \).
(F_q), the subgroup must coincide with the total group. The second part of Theorem 4 is proved in the same way.

3. Symmetric sets of unimodular matrices

Theorem 5. The group of displacements of SM_n(K) is isomorphic to SL_n(K)/{±1} if \( n \geq 3 \) or \( n \geq 2 \) when \( K \neq F_3 \).

Proof. For \( w \in SL_n(K) \) and \( a \in SM_n(K) \), we define a mapping \( T_w \) of \( SM_n(K) \) by \( aT_w = w^t aw \). \( T_w \) is an automorphism of \( SM_n(K) \) since \( w^t (ba^{-1}b)w = (w^t bw)(w^t aw)^{-1} \). If especially \( w = s_1s_2 \) with \( s_1 \) and \( s_2 \) in \( SM_n(K) \), then \( aT_w = s_2(s_1^t a^{-1} s_1^{-1})^{-1}s_2 = a S_{s_1^{-1}} s_{s_2} \), and hence \( T_w = S_{s_1^{-1}} s_{s_2} \). By Theorem 1, \( w \) is a product (of even number) of \( s_i \) in \( SM_n(K) \). Thus \( w \to T_w \) gives a homomorphism of \( SL_n(K) \) onto the group of displacements of \( SM_n(K) \). \( w \) is in the kernel of the homomorphism if and only if \( w^t aw = a \) for every element \( a \) in \( SM_n(K) \). In this case, especially we have \( w^t w = 1 \) or \( w = w^{-1} \). Then \( w^{-1} aw = a \), or \( wa = aw \). Since \( SL_n(K) \) is generated by \( a \), the above implies that \( w \) must be in the center of \( SL_n(K) \). So, \( w = zI \) with \( z \) in \( K \). Then \( w^t w = 1 \) implies \( w^2 = 1 \), or \( z = \pm 1 \). This completes the proof of Theorem 4.

To define \( PSM_n(K) \), we identify elements \( a \) and \( za \) in \( SM_n(K) \) where \( z \) is an element in \( K \) such that \( z^n = 1 \). The set of all classes defined in this way is a symmetric set in a natural way, and we denote it by \( PSM_n(K) \).

Theorem 6. The group of displacements of \( PSM_n(K) \) is isomorphic to \( PSL_n(K) \) if \( n \geq 3 \) or \( n \geq 2 \) when \( K \neq F_3 \).

Proof. Denote by \( a \) an element of \( PSM_n(K) \) represented by \( a \) in \( SM_n(K) \). For \( w \) in \( SL_n(K) \), we define \( T_w : a \to w^t aw \). As before, \( w \to T_w \) gives a homomorphism of \( SL_n(K) \) onto the group of displacements of \( PSM_n(K) \). \( T_w = 1 \) if and only if \( w^t aw = a \) for every \( a \). If \( w \) is in the center of \( SL_n(K) \), then clearly \( T_w = 1 \). So, the kernel of the homomorphism contains the center. On the other hand, we have \[
\begin{bmatrix}
1 & 0 \\
1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}
= \begin{bmatrix}
1 & 1 \\
1 & 2
\end{bmatrix},
\]
which indicates that \( w = \begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix} \oplus I_{n-2} \) is not contained in the kernel. Therefore, the kernel must coincide with the center due to the simplicity of \( PSL_n(K) \). This completes the proof of Theorem 6.

Theorem 7. Suppose that \( n \geq 3 \) or \( n \geq 2 \) if \( K \neq F_3 \). If \( p \neq 2 \) or if \( n \) is odd, then \( SM_n(F_q) \) is transitive. If \( p = 2 \) and \( n \) is even, then \( SM_n(F_q) \) consists of two disjoint ideals, which are transitive.

Proof. First suppose that \( p \neq 2 \) or \( n \) is odd. Then by Theorems 2 and 3, every unimodular symmetric matrix \( a \) is congruent to 1, i.e., \( a = u'u \) with a uni-
modular matrix \( u \). By Theorem 1, \( u \) is a product of even number of unimodular symmetric matrices: \( u = s_1 \cdots s_2 \). Then \( T_n = S_{s_1} S_{s_2} \cdots S_{s_1} \) as in Theorem 6. Then \( a = 1T_n \in 1H \), where \( H \) is the group of displacements. Thus \( SM_n(F_q) \) is transitive in this case. Next suppose that \( p = 2 \) and \( n \) is even. Let \( B_0 \) be the set of all unimodular symmetric matrices with zero diagonal. Elements of \( B_0 \) are congruent to \( j = J \oplus J \oplus \cdots \oplus J \). So, for an element \( a \) in \( B_0 \), there exists \( u \) such that \( u'au = j \). Here \( \det u = 1 \) since \( p = 2 \). By Theorem 4, \( u \) is a product of elements \( a \sim b \) where \( a \) and \( b \) are in \( B_0 \). For \( a \), \( b \) and \( c \) in \( B_0 \), we have \( (b \sim c) a (b \sim c) = a S_{c} S_{c} \), from which we can conclude that \( aH(B_0) \), where \( H(B_0) \) is the group of displacements of \( B_0 \), contains \( j \), and hence \( a \in jH(B_0) \). Thus, \( B_0 \) is transitive. It is also clear that \( J_3 \) is an ideal of \( SM_n(F_q) \) by Theorems 4 and 5. In the same way, we can show that the complementary set of \( B_0 \) in \( SM_n(F_q) \) is an ideal of \( SM_n(F_q) \) and is transitive as a symmetric set.

4. Examples

First of all, we recall the definition of cycles in a finite symmetric set (see [3]). Let \( a \) and \( b \) be elements in a finite symmetric set such that \( a S_{1} S_{2} = a \). Then we call a symmetric subset generated by \( a \) and \( b \) a cycle. To indicate the structure of a cycle, we use an expression: \( a_1 - a_2 \cdots \), where \( a_1 = a \), \( a_2 = b \) and \( a_{i+1} = a_{i-1} S_{a} \) \((i \geq 2)\). If a symmetric set is effective (i.e. \( S_1 = S_2 \) whenever \( c \neq d \)), the above sequence is repetitions of some number of different elements (Theorem 2, [3]). For example, \( a_1 - a_2 \cdots - a_n - a_1 - a_2 \cdots \) where \( a_i \neq a_j \) \((1 \leq i \neq j \leq n)\). In this case, we denote the cycle by \( a_1 - a_2 \cdots - a_n \) and call \( n \) the length of the cycle.

Example 1. \( PSM_3(F_2) \) \((= SM_3(F_2))\).

\( SM_3(F_2) \) consists of the following 28 elements.

\[
\begin{align*}
a_1 & = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_2 & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_3 & = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_4 & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_5 & = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_6 & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_7 & = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_8 & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_9 & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{10} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{11} & = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{12} & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{13} & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{14} & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{15} & = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{16} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{17} & = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{18} & = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{19} & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{20} & = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{21} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{22} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{23} & = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{24} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{25} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{26} & = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{27} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \\
a_{28} & = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},
\end{align*}
\]
We denote $S_{a_i}$ by $S_i$, and a transposition $(a_i, a_j)$ by $(i, j)$. Then each $S_i$ is a product of 12 transpositions as follows.

We list the permutations as follows:

- $S_1 = (3, 4) (5, 8) (6, 7) (9, 28) (11, 12) (13, 16) (14, 15) (17, 27) (19, 20) (21, 24) (22, 23) (25, 26)$,
- $S_2 = (5, 7) (6, 8) (9, 28) (10, 18) (11, 20) (12, 19) (13, 24) (14, 23) (15, 22) (17, 26) (25, 27)$,
- $S_3 = (1, 4) (5, 7) (6, 28) (8, 9) (10, 22) (11, 24) (12, 17) (13, 20) (15, 18) (16, 25) (19, 26) (21, 27)$,
- $S_4 = (1, 3) (5, 8) (6, 7) (9, 10) (11, 27) (12, 21) (13, 26) (14, 18) (16, 19) (17, 24) (20, 25)$,
- $S_5 = (1, 14) (2, 3) (4, 23) (6, 11) (8, 24) (9, 13) (10, 25) (12, 26) (15, 21) (16, 18) (20, 28) (22, 27)$,
- $S_6 = (1, 22) (2, 4) (3, 15) (5, 19) (7, 16) (9, 21) (10, 24) (12, 28) (13, 23) (14, 26) (17, 18) (20, 27)$,
- $S_7 = (1, 23) (2, 3) (4, 14) (6, 13) (8, 20) (9, 11) (10, 21) (15, 25) (16, 22) (17, 19) (18, 27) (24, 28)$,
- $S_8 = (1, 15) (2, 4) (3, 22) (5, 21) (7, 12) (9, 19) (10, 26) (11, 25) (13, 18) (14, 24) (16, 28) (17, 23)$,
- $S_9 = (1, 2) (3, 10) (4, 18) (5, 17) (6, 25) (7, 27) (8, 26) (11, 14) (12, 23) (15, 20) (16, 24) (19, 22)$,
- $S_{10} = (1, 22) (2, 4) (3, 15) (5, 19) (7, 16) (9, 21) (10, 24) (12, 28) (13, 23) (14, 26) (17, 18) (20, 27)$,
- $S_{11} = (1, 22) (2, 21) (3, 23) (4, 9) (5, 19) (7, 16) (9, 21) (10, 24) (12, 28) (13, 15) (14, 27) (16, 17) (20, 26) (22, 28)$,
- $S_{12} = (1, 11) (2, 24) (3, 28) (4, 22) (5, 26) (6, 18) (8, 20) (9, 23) (13, 27) (14, 16) (15, 17) (19, 25)$,
- $S_{13} = (1, 6) (2, 25) (3, 14) (4, 26) (5, 17) (7, 22) (8, 18) (10, 11) (12, 24) (16, 23) (19, 27) (21, 28)$,
- $S_{14} = (1, 21) (2, 23) (4, 27) (5, 24) (6, 26) (7, 11) (8, 15) (9, 18) (10, 12) (13, 20) (17, 22) (19, 28)$,
- $S_{15} = (1, 24) (2, 22) (3, 17) (5, 14) (6, 12) (7, 25) (8, 21) (9, 20) (10, 11) (16, 19) (18, 28) (23, 27)$,
- $S_{16} = (1, 7) (2, 26) (3, 25) (4, 15) (5, 18) (6, 23) (8, 27) (9, 26) (13, 15) (14, 16) (17, 27) (25, 28)$,
- $S_{17} = (1, 12) (2, 21) (3, 23) (4, 9) (5, 19) (7, 16) (9, 21) (10, 24) (12, 28) (13, 15) (14, 27) (16, 17) (20, 26) (22, 28)$,
- $S_{18} = (1, 11) (2, 24) (3, 28) (4, 22) (5, 26) (6, 18) (8, 20) (9, 23) (13, 27) (14, 16) (15, 17) (19, 25)$,
- $S_{19} = (1, 6) (2, 25) (3, 14) (4, 26) (5, 17) (7, 22) (8, 18) (10, 11) (12, 24) (16, 23) (19, 27) (21, 28)$,
- $S_{20} = (1, 21) (2, 23) (4, 27) (5, 24) (6, 26) (7, 11) (8, 15) (9, 18) (10, 12) (13, 20) (17, 22) (19, 28)$,
- $S_{21} = (1, 24) (2, 22) (3, 17) (5, 14) (6, 12) (7, 25) (8, 21) (9, 20) (10, 11) (16, 19) (18, 28) (23, 27)$,
- $S_{22} = (1, 7) (2, 26) (3, 25) (4, 15) (5, 18) (6, 23) (8, 27) (9, 26) (13, 15) (14, 16) (17, 27) (25, 28)$,
- $S_{23} = (1, 12) (2, 21) (3, 23) (4, 9) (5, 19) (7, 16) (9, 21) (10, 24) (12, 28) (13, 15) (14, 27) (16, 17) (20, 26) (22, 28)$,
- $S_{24} = (1, 11) (2, 24) (3, 28) (4, 22) (5, 26) (6, 18) (8, 20) (9, 23) (13, 27) (14, 16) (15, 17) (19, 25)$,
From the above, we can find that for a fixed element there exist two cycles of length 7, three cycles of length 4 and three cycles of length 3 which contain the given element. Also we can find that there are exactly 8 cycles of length 7 in the set given by $C_2$:

$$C_1: 1 - 5 - 14 - 24 - 21 - 15 - 8, \quad C_2: 23 - 5 - 4 - 28 - 10 - 25 - 20, \quad C_3: 11 - 26 - 16 - 21 - 17 - 20, \quad C_4: 6 - 17 - 3 - 12 - 28 - 15 - 18$$

and $C_5$: 7 - 18 - 14 - 9 - 11 - 4 - 27. By observation we see that every element is contained in exactly two of $C_j$ and that conversely any two of $C_i$ have exactly one element in common. Clearly $S_j$ induces a permutation of $C_j$, $j=1, 2, \cdots, 8$, and $S_j$ is uniquely determined by its effect on $C_j$. Now we are going to show that $SM_3(F_2)$ is a simple symmetric set. First, we note that if $t \in C_i$, then there exists $t'$ in $C_i$ such that $t'S_t=t'$. Let $B$ be a quasi-normal symmetric subset. We may assume that $B$ contains 1 ($= a_1$). Suppose that $B$ contains one of $C_1$ or $C_2$, say, $C_1$. For $C_i \neq C_1$, let $s_i = C_i \cap C_i$ and let $t_i$ be such that $t_i \in C_i$ and $t_i \in C_i$. Since there exists $t_i'$ in $C_i$ such that $t_i'S_{t_i}=t_i'$, we have that $BS_{t_i}=B$ by the definition of quasi-normality of $B$. Then $s_iS_{t_i}$ is contained in $B$, which implies that two elements of $C_i$ are contained in $B$. $B$ is a symmetric subset and the length of $C_i$ is 7 (prime), and hence all of the elements in $C_i$ must be in $B$. Thus $B$ must coincide with the total symmetric set. To discuss the general case, we consider all cycles of length 4 and 3 containing 1: $D_1: 1 - 9 - 2 - 28, \quad D_2: 1 - 26 - 18 - 25, \quad D_3: 1 - 27 - 10 - 17, \quad E_1: 1 - 3 - 4, \quad E_2: 1 - 11 - 12, \quad E_3: 1 - 19 - 20$. Clearly, $S_2, S_{10}$ and $S_{18}$ fix the element 1, and we see that $D_1S_{10}=D_2, \quad D_1S_{18}=D_3, \quad D_3S_{18}=D_2, \quad E_1S_{10}=E_2, \quad E_1S_{10}=E_3$ and $E_2S_{18}=E_3$. Therefore, if $B$ contains one of $D_i$, it contains all of $D_i$, and similarly if $B$ contains one of $E_i$, it contains all of $E_i$. In this case, we can verify that $B$ contains one of $C_i$ and hence $B$ must coincide with the total set. Lastly suppose that $B$ which contains 1 contains one of 2, 10 and 18, say, 2. Then $B=BS_{10}$ must contain $2S_{10}=18$, and similarly $B$ contains 10. It is concluded that if $B$ contains one of 2, 10 and 18 then $B$ contains all of them. In this case, $2S_4=2$ implies that $BS_4=B$. So, $B$ contains 1$S_4=3$. Thus $B$ contains $E_i$, and then $B$ coincides with the total set. We have completed the proof that $SM_3(F_2)$ is simple.

**Example 2.** $PSM_2(F_7)$ ($=SM_2(F_7)/\{\pm 1\}$).

This symmetric set consists of the following 21 elements (mod \{± 1\}).

$$a_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a_2 = \begin{bmatrix} 2 & 0 \\ 0 & -3 \end{bmatrix}, \quad a_3 = \begin{bmatrix} 3 & 0 \\ 0 & -2 \end{bmatrix}, \quad a_4 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix},$$

$$a_5 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad a_6 = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}, \quad a_7 = \begin{bmatrix} -3 & 1 \\ 1 & -3 \end{bmatrix}, \quad a_8 = \begin{bmatrix} -1 & 1 \\ 1 & -2 \end{bmatrix},$$
As in Example 1, \( S_j \) stands for \( S_{a_j} \) and \((i, j)\) for \((a_i, a_j)\). Then we have

\[
S_1 = (2, 3) (4, 9) (5, 8) (6, 7) (10, 13) (11, 12) (16, 19) (17, 18), \quad S_2 = (1, 3) (4, 8) (5, 6) (7, 9) (11, 14) (13, 15) (16, 20) (18, 21), \quad S_3 = (1, 2) (4, 6) (5, 9) (7, 8) (10, 15) (12, 14) (17, 21) (19, 20), \quad S_4 = (2, 10) (3, 18) (5, 10) (7, 12) (13, 17) (14, 19) (16, 21), \quad S_5 = (1, 21) (2, 19) (3, 15) (4, 11) (7, 13) (9, 15) (12, 16) (15, 18) (17, 20), \quad S_6 = (1, 7) (2, 19) (3, 8) (4, 14) (9, 15) (12, 20) (13, 21) (16, 17), \quad S_7 = (1, 6) (2, 17) (3, 16) (4, 15) (5, 14) (10, 21) (11, 20) (18, 19), \quad S_8 = (1, 21) (2, 4) (3, 16) (6, 10) (9, 12) (11, 19) (15, 17) (18, 20), \quad S_9 = (1, 20) (2, 17) (3, 5) (6, 11) (8, 13) (10, 18) (14, 16) (19, 21), \quad S_{10} = (1, 13) (3, 15) (4, 11) (7, 21) (8, 14) (9, 18) (12, 17) (16, 20), \quad S_{11} = (1, 12) (2, 14) (5, 10) (7, 20) (8, 19) (9, 15) (13, 16) (17, 21), \quad S_{12} = (1, 11) (3, 14) (4, 15) (5, 16) (6, 20) (8, 13) (10, 19) (18, 21), \quad S_{13} = (1, 10) (2, 15) (4, 17) (5, 14) (6, 21) (9, 12) (11, 18) (19, 20), \quad S_{14} = (2, 11) (3, 12) (4, 19) (6, 10) (7, 13) (9, 16) (15, 20) (17, 18), \quad S_{15} = (2, 13) (3, 10) (5, 18) (6, 11) (7, 12) (8, 17) (14, 21) (16, 19), \quad S_{16} = (1, 15) (2, 10) (4, 21) (5, 12) (6, 17) (7, 8) (9, 14) (11, 18), \quad S_{17} = (1, 14) (3, 11) (4, 13) (5, 20) (6, 16) (7, 9) (8, 15) (10, 19), \quad S_{18} = (1, 14) (2, 12) (4, 6) (5, 15) (7, 19) (8, 20) (9, 10) (13, 16), \quad S_{19} = (1, 15) (3, 13) (4, 14) (5, 6) (7, 18) (8, 11) (9, 21) (12, 17), \quad S_{20} = (2, 10) (3, 13) (4, 9) (5, 17) (6, 12) (7, 11) (8, 18) (14, 21), \quad S_{21} = (2, 12) (3, 11) (4, 16) (5, 8) (6, 13) (7, 10) (9, 19) (15, 20).
\]

It can be verified that we have the following quasi-normal symmetric subsets \( B_i \) which are mapped each other by \( S_{a_i} \) and \((i, j)\) for \((a_i, a_j)\). Then we have \( B_j = \{a_1, a_4, a_{12}\} \), \( B_2 = \{a_3, a_{11}, a_{13}\} \), \( B_3 = \{a_2, a_{12}, a_{17}\} \), \( B_4 = \{a_5, a_{16}, a_{15}\} \), \( B_5 = \{a_7, a_{10}, a_{16}\} \), \( B_6 = \{a_6, a_{13}, a_8\} \), and \( B_7 = \{a_{15}, a_9, a_6\} \). Then we have a homomorphism \( \phi \) of the group generated by all \( S_i \) to the symmetric group of 7 objects \( B_j \) \((j=1, 2, \ldots, 7)\). For example, since \( B_2 S_1 = B_3 \), \( B_2 S_1 = B_5 \) and \( B_4 S_1 = B_4 \) \((k=2, 3, 5, 6)\), we have \( \phi(S_1) = (B_2, B_3) (B_5, B_6) \). Moreover we can see that the homomorphism is into \( A_7 \) (the alternating group). Naturally the homomorphism induces a homomorphism of \( \text{PSL}_2(F_7) \) (= the group of displacements of \( \text{PSM}_2(F_7) \)) into \( A_7 \). Since the former is a simple group, it is an isomorphism onto a subgroup of \( A_7 \). Thus we have shown that \( \text{PSL}_2(F_7) \) is a subgroup of \( A_7 \).

**Example 3.** An ideal in \( \text{SM}_4(F_2) \).

We consider the set of all unimodular symmetric matrices of \( 4 \times 4 \) over \( F_2 \) that
have zero diagonal. It is a symmetric set (an ideal of $SM_4(F_2)$) and consists of the following 28 elements. In the following, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $J = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

$$a_1 = \begin{bmatrix} J & 0 \\ 0 & J \end{bmatrix}, \quad a_2 = \begin{bmatrix} J & 1 & 0 \\ 1 & 0 & J \end{bmatrix}, \quad a_3 = \begin{bmatrix} J & 0 & 0 \\ 0 & 0 & J \end{bmatrix}, \quad a_4 = \begin{bmatrix} J & 0 \\ 0 & J \end{bmatrix},$$

$$a_5 = \begin{bmatrix} J & 0 \\ 0 & J \end{bmatrix}, \quad a_6 = \begin{bmatrix} J & 1 \\ 1 & J \end{bmatrix}, \quad a_7 = \begin{bmatrix} J & 0 \\ 0 & J \end{bmatrix}, \quad a_8 = \begin{bmatrix} J & 1 \\ 1 & 0 \end{bmatrix},$$

$$a_9 = \begin{bmatrix} J & 1 \\ 1 & J \end{bmatrix}, \quad a_{10} = \begin{bmatrix} J & 1 \\ 1 & J \end{bmatrix}, \quad a_{11} = \begin{bmatrix} 0 & 1 \\ J & 0 \end{bmatrix}, \quad a_{12} = \begin{bmatrix} 0 & J \\ J & 0 \end{bmatrix},$$

$$a_{13} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad a_{14} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad a_{15} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad a_{16} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$a_{17} = \begin{bmatrix} 0 & I \\ I & J \end{bmatrix}, \quad a_{18} = \begin{bmatrix} 0 & J \\ J & 0 \end{bmatrix}, \quad a_{19} = \begin{bmatrix} 0 & 1 \\ 1 & J \end{bmatrix}, \quad a_{20} = \begin{bmatrix} 0 & 1 \\ 1 & J \end{bmatrix},$$

$$a_{21} = \begin{bmatrix} 0 & 1 \\ 1 & J \end{bmatrix}, \quad a_{22} = \begin{bmatrix} 0 & 1 \\ 1 & J \end{bmatrix}, \quad a_{23} = \begin{bmatrix} J & I \\ I & 0 \end{bmatrix}, \quad a_{24} = \begin{bmatrix} J & I \\ I & 0 \end{bmatrix},$$

$$a_{25} = \begin{bmatrix} J & 1 \\ 1 & 0 \end{bmatrix}, \quad a_{26} = \begin{bmatrix} J & 1 \\ 1 & 0 \end{bmatrix}, \quad a_{27} = \begin{bmatrix} J & 1 \\ 1 & 0 \end{bmatrix}, \quad a_{28} = \begin{bmatrix} J & 1 \\ 1 & 0 \end{bmatrix}.$$
We can verify that the length of all cycles is three and there exist six cycles which contain a given element. On the other hand, the symmetric set consisting of all transpositions in $S_8$ satisfies the same property. As a matter of fact, we can find an isomorphism $\phi$ of our symmetric set to the latter as follows.

$$
\begin{align*}
\phi(a_1) &= (1, 2), \\
\phi(a_2) &= (4, 7), \\
\phi(a_3) &= (4, 8), \\
\phi(a_4) &= (3, 5), \\
\phi(a_5) &= (3, 6), \\
\phi(a_6) &= (6, 8), \\
\phi(a_7) &= (5, 7), \\
\phi(a_8) &= (5, 8), \\
\phi(a_9) &= (6, 7), \\
\phi(a_{10}) &= (3, 4), \\
\phi(a_{11}) &= (7, 8), \\
\phi(a_{12}) &= (5, 6), \\
\phi(a_{13}) &= (4, 6), \\
\phi(a_{14}) &= (4, 5), \\
\phi(a_{15}) &= (3, 8), \\
\phi(a_{16}) &= (3, 7), \\
\phi(a_{17}) &= (1, 3), \\
\phi(a_{18}) &= (2, 4), \\
\phi(a_{19}) &= (2, 5), \\
\phi(a_{20}) &= (2, 6), \\
\phi(a_{21}) &= (1, 7), \\
\phi(a_{22}) &= (1, 8), \\
\phi(a_{23}) &= (2, 3), \\
\phi(a_{24}) &= (1, 4), \\
\phi(a_{25}) &= (1, 5), \\
\phi(a_{26}) &= (1, 6), \\
\phi(a_{27}) &= (2, 7), \\
\phi(a_{28}) &= (2, 8).
\end{align*}
$$

Since the group of displacements of the symmetric set of all transpositions in $S_8$ coincides with $A_8$, this reestablishes the well known theorem of Dickson that $PSL_4(F_2)$ is isomorphic to $A_8$.

References