<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Simple symmetric sets and simple groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Nobusawa, Nobuo</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 14(2) P.411-P.415</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1977</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/9463">https://doi.org/10.18910/9463</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/9463</td>
</tr>
</tbody>
</table>

**Osaka University Knowledge Archive : OUKA**

https://ir.library.osaka-u.ac.jp/

Osaka University
SIMPLE SYMMETRIC SETS AND SIMPLE GROUPS

Dedicated to the memory of Dr. Taira Honda

Nobuo Nobusawa

(Received December 15, 1975)
(Revised October 12, 1976)

1. Introduction

A binary system \( A \) is called a symmetric set if \( a \circ a = a, (b \circ a) \circ a = b \) and \( (b \circ c) \circ a = (b \circ a) \circ (c \circ a) \). These conditions imply that the right multiplication by an element \( a \), which we denote by \( S_a \) (i.e., \( b \circ a = bS_a \)), is an automorphism of \( A \) of order 2 leaving \( a \) fixed. Note that, if \( \tau \) is an automorphism of \( A \), then \( (b \circ a)\tau = b\tau \circ a\tau \), or \( S_{a\tau} = \tau^{-1}S_a \tau \). Every group is a symmetric set by \( bS_a = ab^{-1}a \). Also the subset of involutions in a group is a symmetric set. For more of symmetric sets, see [3] and [4].

The group of automorphisms of \( A \) generated by all \( S_a \) \( (a \in A) \) is denoted by \( G \), and the subgroup of \( G \) generated by all \( S_aS_e \) \( (a, b \in A) \) is denoted by \( H \). The latter is called the group of displacements. It is easy to see that \( H \) is generated by \( S_aS_e \) \( (e \) is a fixed element and \( a \in A) \). \( H \) is a normal subgroup of \( G \) of index 2. A subset \( B \) of \( A \) is called a symmetric subset if it is closed under the binary multiplication. Every one-point subset is a symmetric subset, and so is \( A \). All the other symmetric subsets are called proper symmetric subsets. A symmetric subset \( B \) is called quasi-normal if \( B\tau \cap B = B \) or \( \phi \) (the empty set) for every element \( \tau \) in \( G \). Now we define a simple symmetric set to be one which has no proper quasi-normal symmetric subset. Theorem and Corollary obtained in 2 state that if \( A \) is simple then \( H \) is either a simple group or a direct product of two simple groups which are conjugate each other in \( G \). If moreover \( A \) is finite, then \( |H| = |A|^2 \) in case \( H \) is not simple. Using this fact, we can show a new proof of the simplicity of the alternating group \( A_n \) \( (n \geq 5) \) in 3 by showing that the subset of all transpositions in \( S_n \) (the symmetric group of \( n \) letters) is a simple symmetric set. This idea is carried out in 4 to obtain examples of simple symmetric sets in vector spaces with bilinear symmetric forms over \( F_2 \), the field consisting of two elements 0 and 1. As special cases, we obtain simple symmetric sets of positive roots of type \( E_6, E_7 \), and \( E_8 \) in Lie algebra theory.
Remark. The above definition of a simple symmetric set is stronger than a standard definition which should be based on non-existence of normal symmetric subsets (See [3]) rather than quasi-normal symmetric subsets. However, the main technique used in this note is to show non-existence of quasi-normal symmetric subsets. So, we keep our definition.

2. The group of displacements of a simple symmetric set

Theorem. If $A$ is a simple symmetric set, then the group of displacements is either a simple group or a direct product of two simple groups which are conjugate each other in $G$.

Proof. First we note that if $A$ is simple then it is transitive, i.e., $A=aG (=aH)$ for an element $a$ in $A$. For, $xG$ for any element $x$ in $A$ is seen to be a quasi-normal symmetric subset and $xG$ can not be equal to $x$ for all $x$ in $A$, and hence $A=aG$ with some element $a$ in $A$. Then of course $A=xG$ for any element $x$ in $A$. Now suppose that $H$ is not simple, and let $N$ be a proper normal subgroup of $H$. Clearly $S_aNS_a=S_bNS_b$ for any $a$ and $b$. Put $N'=S_aNS_a$. $NN'$ and $N\cap N'$ are normal subgroup of $G$ contained in $H$. Generally let $J$ be a normal subgroup of $G$ contained in $H$. Consider $B=eJ$ for an element $e$ in $A$. $B$ is a symmetric subset. Since $B\sigma=eJ\sigma=e\sigma J$ for $\sigma$ in $G$, we have $B\sigma \cap B=B$ or $\phi$, i.e., $B$ is quasi-normal. Since $A$ is simple by the assumption, $eJ=e$ or $A$. If $J=e$, then $eJ=a$ for every element $a$ in $A$, because we have $e\sigma=a$ with some element $\sigma$ in $G$ due to the transitivity of $A$ and then $eJ=\sigma J=\sigma=eJ=\sigma=a$. So, if $eJ=e$, then $J=I$. If $eJ=A$, then, for an arbitrary element $a$ in $A$, $e\sigma=a$ with some element $\sigma$ in $J$. Then $S_a=S_{e\sigma}=\sigma^{-1}S_a\sigma=\tau S_a$ for some element $\tau$ in $J$. This implies that $S_aS_b$ is contained in $J$ for every element $a$ in $A$. Since $H$ is generated by $S_aS_b (a\in A)$, we have $J=H$. Now especially let $J=NN'$. Since $NN'=1$, we have $NN'=H$. Let $J=J\cap J$. Since $N\cap N'\neq H$, we have $N\cap N'=1$. Thus $H$ is a direct product of $N$ and $N'$. Lastly, we show that $N$ is simple. If $M$ is a normal subgroup of $N$, then it is a normal subgroup of $H$. If $M\cap 1$, $H$ is a direct product of $M$ and $S_aMS_a$ as above, which implies $M=N$. Hence $N$ is a simple group.

The author owes the following corollary to Prof. H. Nagao.

**Corollary.** Suppose that $A$ is a finite simple symmetric set. If $H$ is not simple, then $|H|=|A|^2$.

Proof. Suppose that $A$ is finite and simple and that $H$ is not simple. Then $H=N\times N'$ (a direct product) as in Theorem. The mapping $f$ of $A$ in $G$ defined by $f(a)=S_a$ is a homomorphism of symmetric sets. Therefore we can see that $f^{-1}(S_a)$ is a quasi-normal symmetric subset for every $a$ in $A$. 

From this, we can conclude that \( f^{-1}(S_a) = a \) for every element \( a \) and hence \( f \) is a monomorphism. On the other hand, \( A \) is transitive, i.e., \( A = aH \). So, \( f(A) = \{ \sigma^{-1}S \sigma \mid \sigma \in H \} \). Then \( |A| = |f(A)| = |H: C_H(S_a)| \). Here \( C_H(S_a) = \{ \sigma \in H \mid S \sigma = \sigma S \} \). \( H = N \times S_aN \) implies that \( C_H(S_a) = \{ \sigma S_a \sigma S_a \mid \sigma \in N \} \). Thus, \( |C_H(S_a)| = |N| \). Then \( |A| = |H| / |C_H(S_a)| = |N|^2 |N| = |N| \). Therefore, \( |H| = |A|^2 \).

3. Simple symmetric sets in the symmetric groups \( S_n (n \geq 5) \)

Let \( S_n \) be the symmetric group of \( n \) letters where \( n \geq 5 \). Consider the subset \( A \) of \( S_n \) consisting of all transpositions \( (i, j) \) \((1 \leq i < j \leq n)\). \( A \) is a symmetric set. Here \( (i, j)S_{(i, j)} = (p, q) \) where \( p = i^{(r-t)} \) and \( q = j^{(r-t)} \). We show that \( A \) is simple. Let \( B \) be a quasi-normal symmetric subset which contains at least two elements \( a \) and \( b \). Since \( a \neq b \) and \( n \geq 5 \), there exists an element \( c \) in \( A \) such that \( aS_c \neq a \) and \( bS_c = b \). The latter implies that \( BS_c = B \) due to the definition of quasi-normality of \( B \). Then \( aS_c \) is in \( B \). Let \( d = aS_c \). It is easy to see that \( aS_c = d, eS_c = a \) and \( dS_c = c \), i.e., \( a, c \) and \( d \) form a cycle. For example, \( a = (1, 2), c = (2, 3) \) and \( d = (1, 3) \). In this case, for any element \( x \) which is not equal to \( c \), we have that either \( aS_c = a \) or \( dS_c = d \). This implies that \( BS_c = B \) for every element \( x \) in \( A \). On the other hand, we can easily see that \( A \) is transitive. Therefore, \( B = A \) and \( A \) is simple. Clearly, \( |H| \neq |A|^2 \), and hence by Corollary \( H \) is a simple group. Of course, \( H = A \).

Remark. In the above, we can take the set consisting of all \( (i, j) \) \((r, s) \) where \( i, j, r \) and \( s \) are all distinct. The set is also a simple symmetric set, whose order is greater than that of the set given in 3. For example, if we take \( n = 5 \), we get two simple symmetric sets. One has order 10 and the other 15. But both have the same group of displacements which is \( A_5 \).

4. Symmetric sets of vectors over \( F_2 \)

Let \( V \) be a finite dimensional vector space over \( F_2 := \{0, 1\} \). Given a bilinear symmetric form \( Q(x, y) \) on \( V \) with \( Q(x, x) = 0 \), we can give a symmetric structure on \( V \) by defining \( aS_b = a + Q(a, b)b \). In other words, \( aS_b = a \) or \( a + b \) according to \( Q(a, b) = 0 \) or \( \neq 0 \). A cycle in a symmetric set is defined to be a symmetric subset generated by two elements \( x \) and \( y \) such that \( xS_y = x \).

**Proposition 1.** Every cycle in \( V \) has order 3. If \( \{a, b, c\} \) is a cycle, then, for any element \( x \) in \( V \), at least one of \( a, b \) and \( c \) is left fixed by \( S_x \).

Proof. In our case, \( c = a + b \). Then \( Q(c, x) = Q(a, x) + Q(b, x) \). So at least one of \( Q(a, x), Q(b, x) \) and \( Q(c, x) \) is equal to 0.

**Proposition 2.** Let \( A \) be a symmetric subset of \( V \) and \( B \) a quasi-normal sym-
metric subset of $A$. If $B$ contains a cycle, then $BS_x = B$ for every element $x$ in $A$.

Proof. Proposition 2 is a direct consequence of Proposition 1 and the definition of a quasi-normal symmetric subset.

**Proposition 3.** Suppose that $A$ is transitive. Suppose also that, if $xS_y = x$, there exists an element $u$ such that $S_u$ moves one of $x$ and $y$ and leaves the other fixed. Then $A$ is a simple symmetric set.

Proof. Suppose that all the conditions in Proposition 3 are satisfied. Let $B$ be a quasi-normal symmetric subset containing at least two elements $x$ and $y$. If $xS_y = x$, then $BS_y = B$ for every element $a$ in $A$ by Proposition 2. So, assume that $xS_y = x$. Then we have an element $u$ such that, say, $xS_u = x$ and $yS_u = y$. The latter implies that $BS_y = B$. Then $yS_a = B$. This contains a cycle $\{x, y, z\}$, and hence as in former $BS_x = B$ for every element $a$ in $A$. Since $A$ is transitive, we have $B = A$. So, $A$ is simple.

In the following, we take a special $Q$ as follows. Let $Q(x) = \sum_{i, j} x_i x_j$, where $x = (x_1, \ldots, x_n)$. $n = \dim V$. Let $Q(x, y) = Q(x+y) - Q(x) - Q(y)$. Then $Q(x, y) = \sum_{i, j} x_i y_j$. Denote by $V^*$ the set of all non-zero vectors in $V$ and by $V_1$ the set of all vectors $x$ such that $Q(x) = 1$. We also denote by $V^{(i)}$ the set of all vectors that have exactly $i$ non-zero components (i.e., $i$ ones and $n - i$ zeros). For the following examples, also see [1] and [2].

**Example 1.** Let $n = 6$ and $A = V_1$. From the definition of $Q(x)$, we can see that $A = V^{(2)} \cup V^{(3)} \cup V^{(6)}$. First of all we note that $V^{(2)}$ is a symmetric subset which is isomorphic with the symmetric set consisting of transpositions in $S_6$. As a matter of fact, if we denote by $1(i, j)$ the vector which has 1 in the $i$-th and $j$-th positions and 0 everywhere else, the correspondence $1(i, j) \rightarrow (i, j)$ gives the isomorphism of symmetric sets. Elements in $V^{(3)}$ are denoted by $1(i, j, k)$ as above. Then $1(i, j)S_y\{i, j, k\} = 1(i, j)$ if and only if $\{i, j\} \cap \{s, t, u\} = \{r\}$ (one-point set). In this case, $1(i, j)S_y\{i, j, k\} = 1(j, t, u)$ if, say, $i = s = r$. $V^{(6)}$ contains only one element which we denote by $1(1, 2, \ldots, 6)$. Then $1(i, j)S_y\{1, 2, \ldots, 6\} = 1(i, j)$ and $1(i, j, k)S_y\{1, 2, \ldots, 6\} = 1(r, s, t)$ where $\{i, j, k, r, s, t\} = \{1, 2, \ldots, 6\}$. These rules determine the binary operation in $A$. Now we can show that $A$ is a simple symmetric set. For it, we check the conditions in Proposition 3. $A$ is seen to be transitive. Now let $x$ and $y$ be such that $xS_y = x$. If $x$ and $y$ are in $V^{(3)}$, we can easily find $u$ such that $xS_u = x$ and $yS_u = y$. If $x = 1(i, j)$ and $y = 1(r, s, t)$, then $\{i, j\} \cap \{r, x, s\} = \phi$ or, say, $i = r$ and $j = s$. In the former case, let $u = 1(j, k)$ where $k = i, j, r, s, t$. In the latter case, let $u = 1(i, t)$. If $x$ and $y$ are $V^{(3)}$, $xS_y = x$ implies that, if $x = 1(i, j, k)$ and $y = 1(r, s, t)$, then $\{i, j, k\} \cap \{r, s, t\} = \phi$ (one element). We may assume that $i = h = r$. Then let $u = 1(j, g)$ where $\{j, g\} \cap \{r, s, t, k\} = \phi$. When lastly $x = 1(1, 2, \ldots, 6)$ and $y$ any element such that
xS_y=x, it is not difficult to find \( u \) such that \( xS_u=x \) and \( yS_u=y \). Thus we have shown that \( A \) is simple.

Next, we consider basis or generators of \( A \). Clearly, we have generators \( 1(1, 2)=a_1, 1(2, 3)=a_2, 1(3, 4)=a_3, 1(4, 5)=a_4, 1(5, 6)=a_5 \) and \( 1(1, 2, 3)=a_6 \). In a similar sense as Coxeter diagram, we have a diagram

\[
\begin{array}{cccccc}
& a_1 & a_2 & a_3 & a_4 & a_5 \\
\downarrow & & & & & \downarrow \\
& & & a_6 & \end{array}
\]

From this fact, we can show that \( A \) is isomorphic with the symmetric set of positive roots of type \( E_6 \). Note \(|A|=36\). In this case, \( H=\Omega_6(F_2, Q) \). In the following examples, we state the results and details are omitted.

**Example 2.** \( n=6 \) and \( A=V^* \). \( A \) is simple and \(|A|=63\). \( A \) is isomorphic with the set of positive roots of type \( E_7 \). In this case, \( H=PSp_6(F_2) (=Sp_6(F_2)) \).

**Example 3.** \( n=8 \) and \( A=V_1=V^{(2)} \cup V^{(3)} \cup V^{(6)} \cup V^{(7)} \). \( A \) is simple and \(|A|=120\). \( A \) is isomorphic with the set of positive roots of type \( E_8 \). \( H=\Omega_8(F_2, Q) \).

**Example 4.** \( n=8 \) and \( A=V^* \). \( A \) is simple and \(|A|=255\). \( H=PSp_8(F_2) \).

**Example 5.** \( n=10 \) and \( A=V_1=V^{(2)} \cup V^{(3)} \cup V^{(6)} \cup V^{(7)} \cup V^{(10)} \). \( A \) is simple and \(|A|=496\).

**Example 6.** \( n=10 \) and \( A=V^* \). \( A \) is simple and \(|A|=1023\).

**Example 7.** \( n=11 \) and \( A=V^{(2)} \cup V^{(6)} \cup V^{(10)} \). \( A \) is simple and \(|A|=528\).

**Example 8.** \( n=12 \) and \( A=V^{(2)} \cup V^{(6)} \cup V^{(10)} \). \( A \) is simple and \(|A|=1056\).

**University of Hawaii**

---

**References**


