Osaka University Knowledge Archive

Title	On finite homogeneous symmetric sets
Author(s)	Nagao, Hirosi; Nobusawa, Nobuo; Kano, Mikio
Citation	Osaka Journal of Mathematics. 1976, 13(2), p. 399-406
Version Type	VoR
URL	https://doi.org/10.18910/11786
rights	
Note	

Osaka University Knowledge Archive : OUKA

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

Osaka University

Kano, M., Nagao, H. and Nobusawa, N.
Osaka J. Math.
13 (1976), 399-406

ON FINITE HOMOGENEOUS SYMMETRIC SETS

Dedicated to Professor Mutsuo Takahashi on his 60th bitrhday

MIKIO KANO, HIROSI NAGAO AND NOBUO NOBUSAWA

(Received June 19, 1975)

1. Introduction

A symmetric set is a set A on which a binary operation $a\circ b$ is defined satisfying the following three axioms:

(1.1) $a\circ a = a$,

(1.2) $(x\circ a)\circ a = x$,

(1.3) $x\circ(a\circ b) = ((x\circ b)\circ a)\circ b$.

The mapping $S_a\colon A\to A$ defined by $xS_a=x\circ a$ is a permutation on A by (1.2), and it is called the symmetry around a. Corresponding to the axioms above we have the following:

(1.1′) $aS_a = a$,

(1.2′) $S_a^2 = I$,

(1.3′) $S_{a\circ b} = S_{aS_b} = S_b^{-1}S_aS_b$.

We denote by $G(A)$ the permutation group on A generated by $S_A=\{S_a \mid a\in A\}$. Since $T^{-1}S_aT=S_{aT}$ for $a\in A$ and $T\in G(A)$ by (1.3′), S_A is a set of involutions in $G(A)$ which is $G(A)$-invariant. The subgroup of $G(A)$ generated by $\{S_aS_b \mid a, b\in A\}$ is called the *group of displacements* and is denoted by $H(A)$. The set S_A is a symmetric set with binary operation $S_a\circ S_b= S_b^{-1}S_aS_b$. The mapping $a\mapsto S_a$ of A onto S_A is a homomorphism, and if it is an isomorphism, *i.e.* if $a\neq b$ implies $S_a\neq S_b$ then A is called *effective*. If A is effective then the center $Z(G(A))$ of $G(A)$ is trivial.

REMARK. In [4] and [5] the group of displacements is denoted by $G(A)$.

Now suppose that G is a group and A is a subset of G satisfying the following:

(1.4) A is a set of involutions in G which is G-invariant,

(1.5) G is generated by A.

Then A is a symmetric set with the binary operation $a\circ b=b^{-1}ab$, and it is easy to show that $G(A)$ is isomorphic to $G/Z(G)$. If a symmetric set A' is isomorphic to A then we say that A' is *embedded* in a group G. In this case identifying A' with A we regard A' as a set of involutions in G. The subgroup generated by $\{ab \mid a, b\in A\}$ is also called the group of displacements and is denoted by H. If $Z(G)=1$ then A is said to be embedded *faithfully* in G. Every effective symmetric set A is embedded faithfully in the group $G(A)$.

A symmetric set A is called *homogeneous* if it satisfies the following conditions:

(1.6) $a\circ x=b$ has a solution x in A for any $a, b\in A$.

If A is homogeneous then S_A is a conjugate class of involutions in $G(A)$, and the mapping $\phi_a\colon x\mapsto a\circ x$ of A to A is surjective. Now suppose A is finite. Then ϕ_a is also injective, and hence the solution x of $a\circ x=b$ is unique. Especially $aS_x\neq aS_y$ if $x\neq y$. Thus a finite homogeneous summetric set A is effective and can be embedded faithfully in a finite group G. Then the condition (1.6) is equivalent to the following:

(1.7) for any $a, b\in A$ there is $c\in A$ such that $c^{-1}ac=b$.

In this way every finite homogeneous symmetric set A can be regarded as a conjugate class of involutions in a finite group G satisfying (1.5) and (1.7).

The purpose of this paper is to study the structure of finite homogeneous symmetric sets in connection with finite groups generated by a conjugate class of involutions satisfying (1.7). The following theorem, which will be proved in the next section by using the Glauberman's Z^*-Theorem, is fundamental.

Theorem 1. *Suppose a finite symmetric set A is embedded in a group G. Then A is homogeneous if and only if the group of displacements H is of odd order.*

All sets considered in this paper are assumed to be finite. For a set X, $|X|$ denotes the cardinality of X and $|X|_p$ denotes the p-part of $|X|$ for a prime p. For a group G, $O(G)$ denotes the maximal normal subgroup of G of odd order, and $Z^*(G)$ is the subgroup containing $O(G)$ such that $Z^*(G)/O(G)$ coincides with the center of $G/O(G)$. For $a\in G$, the order of a is denoted by $o(a)$. When G acts on a set X the action is called *semiregular* if any $a\neq 1$ of G has no fixed point. Other notation in group theory is the same as in [3].

2. Proof of Theorem 1 and preliminary lemmas

We begin with the following lemma.

Lemma 1. *Let a and b be two involutions in a group G. Then the sub-*

group $\langle a, b\rangle$ *generated by* a *and* b *is the dihedral group of order* $2r$, *where* r *is the order of* ab. *If* $r=o(ab)$ *is odd then* $\langle a, b\rangle-\langle ab\rangle=a\langle ab\rangle$ *is a conjugate class of involutions in* $\langle a, b\rangle$ *satisfying* (1.7).

Proof. Let $x=ab$. Then $\langle a, b\rangle=\langle a, x\rangle$ and we have

$$a^2=1,\quad x^r=1,\quad a^{-1}xa=x^{-1}.$$

Thus $\langle a, b\rangle$ is the dihedral group of order $2r$. If r is odd, then since $x^{-i}ax^i=ax^{2i}$ we have $\{x^{-i}ax^i \mid 0\leqq i<r\}=a\langle x\rangle=\langle a, b\rangle-\langle ab\rangle$. Hence $a\langle x\rangle$ is the conjugate class in $\langle a, b\rangle$ containing a, and for any element c of $a\langle x\rangle$ there is an integer i such that $c=ax^{2i}$. Then $c=(ax^i)^{-1}a(ax^i)$. Since $ax^i\in a\langle x\rangle$, $a\langle x\rangle$ satisfies (1.7).

From now on we assume that A is a symmetric set which is embedded in a group G.

REMARK. For $e, a\in A$, the cycle generated by a with a base point e which is defined in [5] coincides with the following sequence of elements of A:

$$e,\ a=e(ea),\quad e(ea)^2,\quad e(ea)^3, \cdots .$$

Now suppose $H=\langle ab \mid a, b\in A\rangle$ is of odd order. Then by Lemma 1 A satsifies (1.7) and hence A is homogeneous. Thus the "if" part of Theorem 1 is proved.

To prove the "only if" part, we assume that A satisfies (1.7).

Lemma 2. *Under the assumption above we have the following*:

(i) *For* $a, b\in A$ *the element* c *of* A *satisfying* $c^{-1}ac=b$ *is unique.*

(ii) *For* $a\in A$, $A\cap C_G(a)=\{a\}$.

(iii) $|A|$ *is odd.*

(iv) *If* $a, b\in A$ *then* $o(ab)$ *is odd,* $\langle ab\rangle$ *acts on* A *semi-regularly and hence* $o(ab)$ *divides* $|A|$.

(v) *For a fixed* $e\in A$, $H=\langle ea \mid a\in A\rangle=G'$.

(vi) H *is of odd order.*

Proof. (i) By (1.7) the mapping $x\mapsto x^{-1}ax$ of A to A is surjective, and hence injective.

(ii) Since $a^{-1}aa=a$, the assertion follows from (i).

(iii) For $a\in A$, the group $\langle a\rangle$ of order 2 acts on A and it fixes only a. Hence $|A|$ is odd.

(iv) Let $D=\langle a, b\rangle$. Then $\langle a\rangle$ acts on $a^D=\{d^{-1}ad \mid d\in D\}$, and since a fixes only a in a^D, $|a^D|$ is odd. On the other hand $\langle b\rangle$ also acts on a^D, and since $|a^D|$ is odd b fixes an element y of a^D. Then by (ii) $y=b\in a^D$. Hence $b=(ab)^{-i}a(ab)^i=a(ab)^{2i}$ for some i. Thus $(ab)^{2i-1}=1$ and hence $o(ab)$ is odd.

Now suppose $(ab)^{-i}c(ab)^{i}=c$ for some $c\in A$. Then $a^{-1}ca=[(ab)^{i}a]^{-1}c[(ab)^{i}a]$. Since $(ab)^{i}a\in A$ by Lemma 1, we have $a=(ab)^{i}a$ by (i) and hence $(ab)^{i}=1$. Thus if $(ab)^{i}\neq 1$ then $(ab)^{i}$ has no fixed element in A.

(v) For $a, b\in A$, $ab=(ea)^{-1}(eb)$. Hence $H=\langle ab\mid a, b\in A\rangle=\langle ea\mid a\in A\rangle$. Since $G=\langle A\rangle=H\cup eH$, $|G: H|\leqq 2$ and $G'\leqq H$. On the other hand for $a\in A$ there is an element b of A such that $a=b^{-1}eb$, and then $ea=e^{-1}b^{-1}eb\in G'$. Hence $G'=H$.

(vi) Let a be an element of A. Then by (iv), for any $g\in G$, $g^{-1}a^{-1}ga$ is of odd order. Then by the Glauberman's Z^*-Theorem([2], Theorem 1) we have $a\in Z^*(G)$. Since $G=\langle A\rangle$, $G=Z^*(G)$ and hence $O(G)\geqq G'=H$.

The "only if" part of Theorem 1 is proved in (vi) of Lemma 2. Now since G is of even order we have $|G: H|=2$. By the Feit-Thompson's theroem G is solvable and by the Sylow's theroem all involutions are conjugate. Thus we have the following

Corollary. *If a homogeneous symmetric set A is embedded in a group G, then G is solvable, $|G: H|=2$, $|H|$ is odd and A is the only conjugate class of involutions in G.*

Let e be a fixed element of A. Then e induces an involutive automorphism of the group H of odd order. Let $V(e)=C_H(e)$ and $K(e)=\{k\in H\mid e^{-1}ke=k^{-1}\}$. Then we have the following

Lemma 3. (i) *Each coset of $V(e)$ in H contains only one element of $K(e)$, and hence $|H: V(e)|=|K(e)|$.*

(ii) *$K(e)=\{ea\mid a\in A\}$, $|A|=|K(e)|$ and $H=\langle K(e)\rangle$.*

(iii) *If a prime p divides $|H|$ then p also divides $|A|$. In particular if $|A|$ is a power of a prime p then H is a p-group.*

(iv) *Any e-invarian p-subgroup of H is contained in an e-invariant Sylow p-subgroup of H. If P is an e-invariant Sylow p-subgroup of H, then*

$$|A|_p=|K(e)|_p=|P\cap K(e)|,\ |V(e)|_p=|P\cap V(e)|\ .$$

(v) *H is abelian if and only if $H=K(e)$.*

Proof. For the proofs of (i) and (v) see Lemma 2.1 in [1].

(ii) Since A is the conjugate class in G containing e, we have

$$|A|=|G: C_G(e)|=|H: C_H(e)|=|H: V(e)|=|K(e)|\ .$$

Now evindently $\{ea\mid a\in A\}\subseteq K(e)$. Hence we have $K(e)=\{ea\mid a\in A\}$ and $H=\langle K(e)\rangle$.

(iii) If p does not divide $|A|=|K(e)|$, then a Sylow p-subgroup of

$V(e)$ is a Sylow p-subgroup of H. Then by (v) of Lemma 2.1 in [1] p does not divide $|\langle K(e)\rangle|=|H|$, which is a contradiction.

(v) If H is abelian then $K(e)$ is a subgroup, and hence $H=K(e)$. Conversely suppose that $H=K(e)$. Then for $x, y\in H$ $(xy)^{-1}=(xy)^{e}=x^{e}y^{e}=x^{-1}y^{-1}$. Hence x and y commute and H is abelian.

3. Symmetric sets which are also groups

Let X be any group. Then defining the binary operation on X by setting $x\circ y=yx^{-1}y$ X is a symmetric set. In this case we say that the symmetric set X is also a group.

Theorem 2. *Let A be a symmetric set which is also a group. Then A is homogeneous if and only if A is of odd order.*

Proof. If A is homogeneous then by (iii) of Lemma 2 $|A|$ is odd.

Conversely suppose that A is a group of odd order. It suffices to show that the mapping $x\mapsto a\circ x=xa^{-1}x$ is injective, and hence surjective. Since A is of odd order the mapping $x\mapsto x^2$ of A to A is bijective. Let $a=b^2$ and assume $xb^{-2}x=yb^{-2}y$. Then we have $(bx^{-1}b)^2=(by^{-1}b)^2$, $bx^{-1}b=by^{-1}b$ and hence $x=y$.

The following is obtained in [5]. For the completeness we shall prove it in a slightly different way.

Theorem 3. *Let A be an effective symmetric set. Then the following conditions are equivalent:*

(i) *A is also an abelian group.*

(ii) *The group of displacements $H(A)$ is abelian.*

(iii) *$H(A)=\{S_eS_a\,|\,a\in A\}$, where e is a fixed element of A.*

Furtheromre if one of the conditions is satisfied then A is homogeneous and hence $|A|$ is odd.

Proof. (i)$\Rightarrow$(ii) Suppose that A is also an abelian group. Then $a\circ b=ba^{-1}b=a^{-1}b^2$. Since $xS_eS_a=xe^{-2}a^2$, S_eS_a and S_eS_b commute. Hence $H(A)=\langle S_eS_a\,|\,a\in A\rangle$ is abelian

(ii)$\Rightarrow$(iii) Let e be a fixed element of A. Then, since $H(A)$ is abelian and S_e inverts S_eS_a, S_e inverts every element of $H(A)$. Suppose $H(A)$ has an involution T. Then T commutes with S_e, hence T is in the center $Z(G(A))$ of $G(A)$, which is a contradiction. Thus $H(A)$ is of odd order, and by Theorem 1 A is homogeneous. By (v) of Lemma 3 we have $H(A)=\{S_eS_a\,|\,a\in A\}$.

(iii)$\Rightarrow$(i) Suppose $H(A)=\{S_eS_a\,|\,a\in A\}$. Since S_e inverts every element of $H(A)$, $H(A)$ is an abelian group. Then it is easy to see that the mapping $a \mapsto S_e S_a$ of A onto $H(A)$ is an isomorphism of symmetric sets. Thus A is also an abelian group.

The last half of the theorem has been shown in the proof of (ii)$\Rightarrow$(iii).
A symmetric set A is called *abelian* if $H(A)$ is abelian group.

4. Symmetric subsets

Let A be a symmetric set. A subset B of A is called a *symmetric subset* of A if $b \circ c \in B$ for any $b, c \in B$. If B is a symmetric subset of A then $B \circ a$ is also a symmetric subset, and if A is homogeneous then B is also homogeneous and $B \cap B \circ a = \phi$ for $a \in A - B$.

From now on we assume that A is a homogeneous symmetric set which is embedded in a group G, and let $H = \langle ab \mid a, b \in A \rangle$. If B is a symmetric subset of A then B is embedded in $G_B = \langle B \rangle$. Let $H_B = \langle bc \mid b, c \in B \rangle$.

Theorem 4. (i) *Let B be a subset of A and $e \in B$. Then B is a symmetric subset if and only if there exists an e-invariant subgroup J of H such that $B = e^J = \{j^{-1}ej \mid j \in J\}$.*

(ii) *A symmetric subset B is abelian if and only if there exists an e-invariant abelian subgroup J of H scuh that $B = e^J$.*

Proof. If B is a symmetric subset of A, then $H_B = \langle eb \mid b \in B \rangle$ is e-invariant and $B = e^{H_B}$. By Theorem 3 B is abelian if and only if H_B is abelian. Suppose conversely that J is an e-invariant subgroup of H and $B = e^J$. Then for $j, k \in J$ $e^j \circ e^k = e^{-k} e^j e^k = k^{-1}(jk^{-1})^{-e} e (jk^{-1})^e k \in e^J$. Hence B is a symmetric subset.

Theorem 5. *If B is a symmetric subest of a homogeneous symmetric set A, then $|B|$ divides $|A|$.*

Proof. Let $e \in B$ and p a prime division of $|B|$. By (iv) of Lemma 3 there is an e-invariant Sylow p-subgroup Q of H_B and Q is contained in an e-invariant p-subgroup P of H. Then

$$|A|_p = |P \cap K(e)|_p \geqq |Q \cap K(e)|_p = |B|_p .$$

Hence $|B|$ divides $|A|$.

A symmetric subset B of A is called a symmetric p-subset if $|B|$ is a power of p, and B is called a *symmetric Sylow p-subset* if $|B| = |A|_p$. Then we have the following Sylow's theorem for homogeneous symmetric sets.

Theorem 6. *Let C be a symmetric p-subset of a homogeneous symmetric set A. Then C is contained in a symmetric Sylow p-subset of A. Two symmetric*

Sylow p-subsets of A are isomorphic.

Proof. Let $e \in C$. By (iii) of Lemma 3 H_C is an e-invariant p-subgroup of H and is contained in an e-invariant Sylow p-subgroup P of H. Let $B = e^P$. Then $C = e^{H_C} \subseteq B$, and since

$$|B| = |P : P \cap V(e)| = |P \cap K(e)| = |A|_p$$

B is a symmetric Sylow p-subset of A.

Now let B' be any symmetric Sylow p-subset of A. Then there is an element a of A such that $B'^a \ni e$. Let $B'' = B'^a$. Then $H_{B''}$ is an e-invariant p-subgroup and is contained in an e-invariant Sylow p-subgroup P'' of H. Since $B'' = e^{H_{B''}} \leqq e^{P''}$ and $|B''| = |A|_p = |e^{P''}|$, we have $B'' = e^{P''}$. By (ii) of Theorem 2.2 in [3], Chapter 6 there is an element x of $C_H(e)$ such that $P'' = P^x$. Then $B'' = e^{P''} = (e^P)^x = B^x$ and hence $B' = (B'')^a = B^{xa}$. Thus B' is isomorphic to B.

5. Symmetric quotient sets

Suppose that an equivalence relation $\sim$ in a symmetric set A satisfies the following condition: if $a \sim a'$ and $b \sim b'$ then $a \circ b \sim a' \circ b'$. Denote the equivalence class containing a by a^*. Then the set of all equivalence classes $A^* = A/\sim$ is a symmetric set with the binary operation $a^* \circ b^* = (a \circ b)^*$. We call A^* a *symmetric quotient set* of A and an equivalence class is called a *coset*. Since $b \circ c \sim a \circ a = a$ for $b, c \in a^*$, each coset is a symmetric subset of A.

Now suppose A is homogeneous. Then a symmetric quotient set A^* of A is also homogeneous. Let $e \in A$ and $B = e^*$. If $x \sim e \circ a$ then $x \circ a \sim (e \circ a) \circ a = e$ and hence $x = (x \circ a) \circ a \in B \circ a$. Thus $(e \circ a)^* \subseteq B \circ a$. On the other hand if $b \sim e$ then $b \circ a \sim e \circ a$. Hence $B \circ a \subseteq (e \circ a)^*$ and we have $(e \circ a)^* = B \circ a$. Since A is homogeneous every coset can be written in a form $B \circ a$ with $a \in A$. Therefore A^* is uniquely determined by a coset B, and hence we may denote A^* by A/B. A symmetric subset B of A is called *normal* in A if B is a coset of some symmetric quotient set of A.

Let A be a homogeneous symmetric set embedded in a group $G, H = \langle ab \mid a, b \in A \rangle$ and $e \in A$. If J is a subgroup of H which is normal in G, then $\bar{A} = A \bmod J$ is a symmetric set which is homomorphic to A, and $\bar{A}$ is embedded in $\bar{G} = G/J$. Then the group of its displacements is $\bar{H} = H/J$.

Theorem 7. (i) *Let B be a symmetric subset of A containing e. Then B is normal in A if and only if there exists a normal subgroup J of G such that $J \subseteq H$ and $B = e^J$. In this case A/B is isomorphic to $\bar{A} = A \bmod J$.*

(ii) *Let B be a symmetric normal subset of A. Then A/B is abelian if and only if there exists a normal subgroup J of G such that $B = e^J, J \subseteq H$ and H/J is abelian.*

Proof. Suppose first that J is a normal subgroup of G contained in H. Let $\bar{G}=G/J$ and $\bar{A}=\{\bar{a}=aJ \mid a\in A\}$. Let $a^*=\{b\in A \mid \bar{b}=\bar{a}\}$. Then $A^*=\{a^* \mid a\in A\}$ is a symmetric quotient set of A and $A^*\simeq\bar{A}$. Suppose $\bar{a}=\bar{b}$ for $a, b\in A$. Then $b=aj$ with $j\in J$, and since a and b are involutions $a^{-1}ia=j^{-1}$. Since J is of odd order there is an element i of J such that $i^2=j$. Then $a^{-1}ia=i^{-1}$ and we have $b=i^{-1}ai\in a^J$. Conversely if $b\in a^J$ then $\bar{a}=\bar{b}$. Thus we have $a^*=a^J$ and a^J is a coset. By Theorem 3 $\bar{A}(\simeq A^*=A/e^J)$ is abelian if and only if $\bar{H}=H/J$ is an abelian group.

Suppose next that $B=e^*$ is a coset of a symmetric quotient set A^* of A.

If $a^*=b^*$ then for $c\in A$ $(a^c)^*=(b^c)^*$, and hence $(a^x)^*=(b^x)^*$ for any $x\in G$. Since $B^a=B^b$ we have $B^{ab}=B$. Let $J=\langle ab \mid a, b\in A,\ a^*=b^*\rangle$. Then J is a normal subgroup of G contained in H and $e^J\subseteq B$. Since $H_B=\langle eb \mid b\in B\rangle\leqq J$, and $B=e^{H_B}$, we have $e^J=B$.

By using the solvability of H, we have the following

Corollary 1. *If A is a homogeneous symmetric set, then there is a chain of symmetric subsets*

$$A = B_0\supset B_1\supset\cdots\supset B_n = \{e\}$$

such that B_{i+1} is normal in B_i and B_i/B_{i+1} is abelian.

Let Z be the center of H. Then Z is clearly a normal subgroup of G and hence by Theorem 7 e^Z is a normal symmetric subset of A which is abelian by (ii) of Theorem 4. In [4] e^Z is called the center of A(relative to a base point e). Now suppose that A is faithfully embedded in G. Then $|e^Z|=|Z|$. If A is a symmetric p-set then H is a p-group by (iii) of Lemma 3 and hence H has a non-trivial center. Thus we have

Corollary 2. *If A is a homogeneous symmetric p-set, then the center of A relative to a base point e is not trivial.*

AKASHI TECHNICAL COLLEGE
OSAKA UNIVERSITY
UNIVERSITY OF HAWAII

References

[1] H. Bender: *Transitive Gruppen gerader Ordnung in denen jede Involution genau einen Punkt festlässt*, J. Algebra **17** (1971), 527–554.
[2] G. Glauberman: *Central elements in cone-free groups*, J. Algebra **4** (1966), 403–420.
[3] D. Gorenstein: Finite Groups, Harper and Row, New York, 1968.
[4] O. Loos: Symmetric Spaces I, Benjamin, New York, 1969.
[5] N. Nobusawa: *On symmetric structure on a finite set*, Osaka J. Math. **11** (1974), 569–575.