



Title	On symmetric structure of a finite set
Author(s)	Nobusawa, Nobuo
Citation	Osaka Journal of Mathematics. 1974, 11(3), p. 569-575
Version Type	VoR
URL	https://doi.org/10.18910/12492
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

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

The University of Osaka

ON SYMMETRIC STRUCTURE OF A FINITE SET

NOBUO NOBUSAWA

(Received December 17, 1973)

(Revised April 5, 1974)

1. Introduction

A symmetric structure of a finite set A is defined to be a mapping S of A into the group of permutations on A (the image of an element a in A by S is denoted by S_a or by $S[a]$ and the image of an element b in A by a permutation S_a is denoted by bS_a) such that (i) $aS_a = a$, (ii) $S_a^2 = I$ (the identity permutation) and (iii) $S[bS_a] = S_a S_b S_a$ for a and b in A . A set with a symmetric structure is called a symmetric set (with a given symmetric structure). Every group G has a symmetric structure S defined by $bS_a = ab^{-1}a$ for a and b in G , and when we regard a group as a symmetric set we always take this symmetric structure. Generally a symmetric set has a more complicate structure than a group and to develop a structure theory of a symmetric set seems to be an open problem. In this note, we first investigate the following two conditions.

(E) $S_a \neq S_b$ if $a \neq b$.

(H) For any elements a and b , there exists an element c such that $aS_c = b$.

Symmetric sets which satisfy (E) (or (H)) are called *effective* (or *homogeneous*).

Proposition 1. (H) implies (E).

Proof. Suppose that (H) is satisfied. Fix an element a and consider a correspondence $b \rightarrow b'$ defined by $aS_b = b'$. The correspondence is a surjective mapping of A to A due to (H). Since A is a finite set, it is a bijection. Therefore, if $b \neq c$, then $aS_b \neq aS_c$. Naturally $S_b \neq S_c$.

Actually (H) is stronger than (E).

EXAMPLE 1. Let $A = \{1, 2, 3, 4, 5, 6\}$. Consider S defined by $S_1 = (24)(36)$, $S_2 = (14)(35)$, $S_3 = (25)(16)$, $S_4 = (56)(12)$, $S_5 = (23)(46)$ and $S_6 = (45)(13)$. S is a symmetric structure of A . (E) is satisfied but not (H), since 1 is not mapped to 4 by any S_i .

Next, we consider the group of displacements of A , which is defined to be a subgroup of the group of permutations on A generated by $S_a S_b$ for all a and b in A . Denote it by $G(A)$.

Proposition 2. Fix an element e in A and consider a mapping of A to $G(A)$ defined by $a \rightarrow S_e S_a$. Then the mapping is a homomorphism of a symmetric set A to a symmetric set $G(A)$.

Proof. Let S' be the symmetric structure of a group $G(A)$. We have to show that aS_b is mapped to $(S_e S_a)S'[S_e S_b]$. Now aS_b is mapped to $S_e S[aS_b]$ which is equal to $S_e S_b S_a S_b = S_e S_b S_a S_e S_b = S_e S_b (S_e S_a)^{-1} S_b S_e = (S_e S_a)S'[S_e S_b]$ as we claimed.

If A is effective, then the homomorphism in Proposition 2 is an isomorphism of A into $G(A)$, and hence in this case a symmetric set A is regarded as a subset of a group closed under the operation $ab^{-1}a$. Note also that $G(A)$ is generated by $S_e S_a$ (a in A) as $S_a S_b = S_a S_e S_e S_b$ and $S_a S_e = (S_e S_a)^{-1}$. In 3, it will be proved that an effective symmetric set is isomorphic with $G(A)$ if and only if $G(A)$ is abelian. (cf. Proposition 2.5. p. 137 [2]) One of the basic concepts in studying the structure of a symmetric set is a cycle which will be defined in 2 as a generalization of a cyclic subgroup of a group. The structure of a cycle will be completely determined in 2. In 4, we shall show that a homogeneous symmetric set of p^2 elements where p is an odd prime is isomorphic with an abelian group, but in 5 we shall show that there is a homogeneous symmetric set of 27 elements which is not isomorphic with a group. In 6, we shall give a complete table of symmetric structures of a set of 5 elements. It would be a rather complicate work to find a complete table of symmetric structures of a set of more than 5 elements.

2. Cycles

Fix an element e in A . For an element a in A , we define

$$a^k = \begin{cases} e(S_e S_a)^i & \text{if } k = 2i \\ a(S_e S_a)^i & \text{if } k = 2i+1. \end{cases}$$

From now on, we shall denote $S_e S_a$ by U_a . Clearly, $U_a^{-1} = S_a S_e$ and $S[bU_a] = U_a^{-1} S_b U_a$.

Proposition 3. $S[a^k] = S_e U_a^k$.

Proof. First suppose $k=2i$. Then $S[a^k] = S[eU_a^i] = U_a^{-i} S_e U_a^i = (S_a S_e)^i S_e U_a^i = S_e S_e (S_a S_e)^i S_e U_a^i = S_e U_a^i S_e S_e U_a^i = S_e U_a^{2i} = S_e U_a^k$. Next, suppose $k=2i+1$. Then $S[a^k] = S[aU_a^i] = U_a^{-i} S_a U_a^i = (S_a S_e)^i S_a U_a^i = S_e S_e (S_a S_e)^i S_a U_a^i = S_e U_a^{i+1+i} = S_e U_a^k$.

Proposition 4. $a^j S[a^k] = a^{-j+2k}$. Especially $a^j S[a^{j+1}] = a^{j+2}$.

Proof. $a^j S[a^k] = a^j S_e U_a^k$ by Proposition 3. Suppose $j=2i$. Then $a^j S_e U_a^k = e(S_e S_a)^i S_e U_a^k = e S_e (S_a S_e)^i (S_e S_a)^k = e U_a^{-i+k} = a^{-2i+2k} = a^{-j+2k}$. Suppose $j=2i+1$.

Then $a^j S[a^k] = a(S_e S_a)^i S_e U_a^k = a S_a (S_e S_a)^i S_e U_a^k = a U_a^{-i-1} U_a^k = a U_a^{-i-1+k} = a^{2(-i-1+k)+1} = a^{-j+2k}$.

Now consider a sequence e, a, a^2, a^3, \dots . The latter part of Proposition 4 implies that in the sequence the succeeding element of an element, say, b in the sequence is an image of the preceding element by S_b . We call such a sequence a cycle (generated by a with a base element e). Later we shall consider a set of all distinct elements in a cycle and call it also a cycle. Let $\text{ord}_e a$ (or simply $\text{ord } a$ if the base element e is implicitly pregiven) be the least positive integer n such that $a^n = e$, the existence of which is given in the following proposition.

Proposition 5. *There exists $\text{ord } a$, and if we denote it by n and $\text{ord } U_a$ (the order of a permutation U_a) by m , then $n=m$ or $2m$. If (E) holds, then $n=m$.*

Proof. $a^{2m} = e U_a^m = e$, and so $n \leq 2m$. On the other hand, by Proposition 3, $U_a^n = S_e S[a^n] = S_e S_e = I$. So m divides n . Therefore $n=m$ or $2m$. We have $I = U_a^m = S_e S[a^m]$, which implies that $S[a^m] = S_e$. Therefore, $a^m = e$ or $n=m$ if (E) holds.

From now on, we shall denote $n = \text{ord } a$ and $m = \text{ord } U_a$.

Theorem 1. *If $i \equiv j \pmod{2m}$, then $a^i = a^j$. Conversely if $a^i = a^j$, then $i \equiv j \pmod{m}$.*

Proof. If $i \equiv j \pmod{2m}$, then $a^i = a^j$ by definition of a^k . Suppose that $a^i = a^j$. Then $U_a^i = U_a^j$ by Proposition 3, whence $i \equiv j \pmod{m}$.

Corollary. *$a^k = e$ if and only if $k \equiv 0 \pmod{n}$.*

Proof. By Theorem 1, a cycle e, a, \dots consists of repetitions of e, a, \dots, a^{2m-1} . So if $n=2m$, Corollary is clear. Suppose $n=m$. We have to show that if $a^i = e$ for $0 < i < 2m$ then $i=n$. But, by Theorem 1, if $a^i = e$ then $i \equiv 0 \pmod{m}$ ($=n$). Therefore $i=n$.

So far we have seen that a cycle e, a, \dots consists of repetitions of e, a, \dots, a^{n-1} or of repetitions of e, a, \dots, a^{2n-1} . When we have the former case, we call the cycle *regular*.

Theorem 2. *If n is odd or if $n=2m$, then a cycle e, a, \dots is regular. If (E) holds, then every cycle is regular.*

Proof. The last statement is clear because $a^i = a^j$ if and only if $S[a^i] = S[a^j]$ when (E) holds, i.e., if and only if $i \equiv j \pmod{m}$ ($=n$). Next suppose $n=2k+1$. To show the regularity of the cycle, it is sufficient to show that $a^{n+1} = a$. Now $a^{n+1} = a^{2k+2} = a^{2(k+1)} = e U_a^{k+1}$. Since $e = a^n = a U_a^k$, we have that $e U_a^{k+1} = a U_a^k U_a^{k+1} = a U_a^{2k+1} = a U_a^n = a$. Here note that in this case $n=m$ because n is odd. If $n=2m$, then the cycle is clearly regular.

Corollary. $a^{n+2k}=a^{2k}$.

Proof. If the cycle is regular, there is nothing to prove. So we may suppose by Theorem 2 that n is even and $n=m$. Then $a^{n+2}=a^n S[a^{n+1}]=e S_e U_a^{n+1}=e U_a=a^2$. Now consider a cycle e, a^2, a^4, \dots . It consists of repetitions of e, a^2, \dots, a^{n-2} . This completes the proof of Corollary.

EXAMPLE 2. Let $A=\{1, 2, \dots, 6\}$. Define $S_1=(26)(45)$, $S_2=(13)(46)$, $S_3=(24)(56)$, $S_4=(13)(25)$, $S_5=S_2$ and $S_6=S_4$. S is a symmetric structure of A . We have a cycle $1, 2, 3, 4, 1, 5, 3, 6, 1, 2, \dots$. The cycle is not regular. A is not effective and $n=m=4$.

The following proposition will be used in 3.

Proposition 6. *A symmetric set A is homogeneous if and only if $\text{ord}_e a$ is odd for any e and a in A .*

Proof. Let C be a subset of A consisting of all distinct elements of e, a, \dots . C is also called a cycle. C is a symmetric set with a symmetric structure induced from that of A . Generally we call such a subset as a symmetric subset of A . If A is homogeneous, then every symmetric subset B of A is also homogeneous as is seen from the proof of Proposition 1. So if A is homogeneous, then C is so. Then $\text{ord } a$ must be odd. Otherwise, $n=2k$ and $S[a^k]=S_e$ since $a^t S[a^k]=a^{-t+2k}=a^{-t}=a^t S_e$ but then $a^k=e$ (a contradiction). Conversely suppose that $\text{ord } a$ is odd for any e and a . Put $\text{ord } a=2k+1$. Consider an element $b=a^{k+1}$, and we see that $a S_b=a^{-1+2(k+1)}=a^{2k+1}=e$ by Proposition 4. Thus a is mapped to e . But a and e are taken arbitrarily in A . So (H) is satisfied.

3. Abelian symmetric sets

A is called abelian if $G(A)$ is abelian.

Lemma. *Let e, a and d be elements in an abelian symmetric set A . Put $d^{(k)}=d U_a^k$. Then $d, d^{(1)}, d^{(2)}, \dots$ is a cycle. If $m(=\text{ord } U_a)=2j$, then $\text{ord } S_a S[d^{(1)}]=j$.*

Proof. $S_a S[d^{(1)}]=S_a S[d U_a]=S_a S_a S_e S_a S_e S_a$. But $S_a S_e S_a=S_a S_e S_a$ since $S_e S_a S_e S_a=S_e S_a S_e S_a$ for $G(A)$ is abelian. Therefore, $S_a S[d^{(1)}]=S_a S_a S_e S_a S_e S_a=U_a^2$, and hence $\text{ord } S_a S[d^{(1)}]=j$ if $\text{ord } U_a=2j$. Now if $k=2i$, then $d^{(k)}=d U_a^{2i}=d(S_a S[d^{(1)}])^i$, and if $k=2i+1$, then $d^{(k)}=d U_a^{2i+1}=d^{(1)} U_a^{2i}=d^{(1)}(S_a S[d^{(1)}])^i$. This shows that $d, d^{(1)}, d^{(2)}, \dots$ is a cycle.

Theorem 3. *An effective abelian symmetric set is homogeneous.*

Proof. Suppose that A is abelian and effective. By Proposition 6, we have to show that $\text{ord } a$ is odd. Assume on the contrary that $\text{ord } a=2j$. Due

to (E), $m(=\text{ord } U_a)=n=2j$. Therefore, $j < m$ or $U_a^j \neq I$. Then there exists an element d such that $dU_a^j \neq d$. On the other hand, if we apply the above lemma on d , we have a cycle $d, d^{(1)}, \dots$ such that $\text{ord } S_a S[d^{(1)}]=j$. Due to (E), $\text{ord } S_a S[d^{(1)}]=\text{ord}_a d^{(1)}$. Thus $d^{(j)}=d$. This is a contradiction.

Theorem 4. *Let A be an effective symmetric set. Then A is abelian if and only if $G(A)=\{S_e S_a \mid a \text{ in } A\}$ for an element e in A .*

Proof. First suppose that A is abelian. By the proof of Theorem 3, $\text{ord } a=2k+1$ (odd). Then $e=a^{2k+1}=aU_a^k$, and so $eU_a^{k+1}=aU_a^k U_a^{k+1}=aU_a^{2k+1}=a$. Therefore, $a^{2k+2}=a$, or $a^{2t}=a$ with $t=k+1$. Then $S_b S_e S_a=S_b S_e S[a^{2t}]=S_b S_e S[eU_a^t]=S_b S_e (S_a S_e)^t S_e (S_e S_a)^t=(S_a S_e)^t S_b S_e S_e (S_e S_a)^t=(S_a S_e)^t S_b (S_e S_a)^t=S_e$ with $c=bU_a^t$. This implies that $S_e S_b S_e S_a=S_e S_c$. Also we have that $(S_e S_a)^{-1}=(S_e S_a)^{m-1}=S_e S_d$ with $d=a^{m-1}$. Every element of $G(A)$ is a product of $S_e S_a$ (a in A). Then the above result shows that every element of $G(A)$ is expressed as $S_e S_a$ with an element a in A . As to the converse, note that $G(A)$ has an automorphism (as a group) defined by $T \rightarrow S_e T S_e$ with a fixed element e . If $G(A)=\{S_e S_a \mid a \text{ in } A\}$, then the automorphism maps every element of $G(A)$ to its inverse. In such a case, a group must be abelian. (The converse part of Theorem 4 is pointed out by Prof. H. Nagao.)

4. Homogeneous symmetric sets of p^2 elements

Let A be a symmetric set and C a symmetric subset of A . Moreover, suppose that C is a cycle $\{e, a, \dots, a^{t-1}\}$ where $t=\text{ord } a$. We denote $\{S_e S[a^i] \mid i=0, 1, \dots, t-1\}$ by $G'(C)$. $G'(C)$ is a cyclic subgroup of $G(A)$. Now suppose that A is homogeneous. For an element b in A , $bG'(C)$ consists of t elements because $bS_e S[a^i]=bS_e S[a^j]$ implies $a^i=a^j$ by the proof of Proposition 1. If d is an element in A , then $bG'(C)$ and $dG'(C)$ are either identical or disjoint as $G'(C)$ is a group. Thus A is a set-theoretical union of disjoint subsets $bG'(C)$, $b'G'(C), \dots$. This proves the following.

Proposition 7. *Let A be a homogeneous symmetric set of k elements and C a symmetric subset of t elements which is a cycle. Then t divides k .*

Now let A be a homogeneous symmetric set of p^2 elements where p is an odd prime. If A is a cycle, it is naturally abelian and is isomorphic with a cyclic group. So, assume that A is not a cycle. By Proposition 7, every non-trivial cycle consists of p elements. From now on, we are going to use some geometric terms. Call an element in A a point. A cycle is said to be passing through a point if it contains the point. Then we can show that there is one and only one cycle passing through given two points as p is a prime. Two cycles are said to be parallel if they have no point in common. Next we shall show that, if a point a is not contained in a cycle C , then there is one and only one cycle passing through

a and parallel to C . To see it, we first note that the number of cycles passing through a point is $(p^2-1)/(p-1)=p+1$. Now there are p cycles passing through a and points in C . Thus we have the above fact. Then, if C_1 is parallel to C_2 and C_2 to C_3 (C_i are all different cycles), C_1 is then parallel to C_3 . By counting the number again, we conclude that there are exactly p cycles which are parallel each other. Now fix a point e in A . Let D_0 be a cycle $\{e, a, \dots, a^{p-1}\}$. Let C_i be cycles passing through a^i and parallel to C_0 ($i=0, 1, \dots, p-1$). Let C_0 be $\{e, b, \dots, b^{p-1}\}$, and D_j cycles passing through b^j and parallel to D_0 ($j=0, 1, \dots, p-1$). We shall show that $C_i S_d = C_k$ for $i \neq k$ if and only if d is in C_j where $k \equiv 2j - i \pmod p$. First, we have that $C_i S[a^j] = C_k$ since $C_i S[a^j]$ contains a^k and is parallel to C_i . (If $C_i S[a^j]$ and C_i intersect at a point c , then $c = c' S[a^j]$ with a point c' in C_i which implies that a^j is in C_i .) Now consider a set $F = \{u \text{ in } A \mid C_i S_u = C_k\}$. It is not hard to show that F is a symmetric subset of A and is parallel to C_i . Since F contains a^j , $F = C_j$. Similarly $D_i S_d = D_k$ for $i \neq k$ if and only if d is in D_j where $k \equiv 2j - i \pmod p$. Now every point in A is determined as an intersection point of C_i and D_j for some i and j . Denote the point by $u(i, j)$. Then we have by the above result that $u(i, i') S[u(j, j')] = u(k, k')$ where $k \equiv 2j - i$ and $k' \equiv 2j' - i' \pmod p$. Thus A is isomorphic with a group which is a direct product of two cyclic groups of order p .

5. A homogeneous set of 27 elements

Let $A = \{1, 2, \dots, 9, 1', 2', \dots, 9', 1'', 2'', \dots, 9''\}$. Define S as follows. $iS_k = 2k - i$, $i'S_k = (i+k)''$, $i''S_k = (i-k)'$; $iS_{k'} = (i+k)''$, $i'S_{k'} = (2k-i)'$, $i''S_{k'} = i-k$; $iS_{k''} = (k-i)'$, $i'S_{k''} = k-i$, $i''S_{k''} = (2k-i)''$. Here all integers are considered mod 9. By routine computations we can verify that S is a symmetric structure of A satisfying (H). For example, we have to check that $S_{k''} S_i S_{k'} = S[tS_{k''}] = S[(k-t)']$. But the both left and right sides of the above will map i to $(k-t+i)''$, i' to $(2k-2t-i)'$, and i'' to $-k+t+i$, and hence we have the identity. A is not isomorphic with a group, because there is one and only one cycle of order 9 passing through a point, say, 1; namely, $\{1, 2, \dots, 9\}$. On the other hand, in a group of order 27, taking the group identity e , we can see that either there is no cycle (in this case cyclic subgroup) of order 9 passing through e or else there are more than one cycle of order 9 passing through e . (See p. 52 [1].)

6. A table of symmetric structures of a set of 5 elements

The following is a complete table of symmetric structures of a set of 5 elements 1, 2, \dots , 5. There are 14 types including a trivial case.

Type	S_1	S_2	S_3	S_4	S_5
1	(25) (34)	(13) (45)	(24) (15)	(35) (12)	(14) (23)
2	(24)	(13)	(24)	(13)	I
3	(24)	(13)	(24)	(13)	(13)
4	(24)	(13)	(24)	(13)	(13) (24)
5	(23)	(13)	(12)	I	I
6	(23) (45)	(13)	(12)	I	I
7	(23) (45)	(13) (45)	(12) (45)	I	I
8	(23)	I	I	I	I
9	(23) (45)	I	I	I	I
10	(23)	I	I	(23)	I
11	(23)	(45)	(45)	I	I
12	(23)	I	I	(23)	(23)
13	(23) (45)	(45)	(45)	I	I
14	I	I	I	I	I

UNIVERSITY OF HAWAII

References

- [1] M. Hall jr: Theory of Groups, Macmillan, New York, 1959.
- [2] O. Loos: Symmetric Spaces; Vol. 1, Benjamin, New York, 1969.

