SOME ELEMENTARY CONCEPTS OF PERMUTATION GROUPS

by

WILLIAM V. MADDEN

B. S., South Dakota State College, 1963

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1965

Approved by:

Robert Bechtel

Major Professor

TABLE OF CONTENTS

INTRODUCTION

This report is concerned with particular mappings of sets and various properties of these mappings. Sets will be denoted by capital Roman letters; objects in a set by the letters a,b..., or merely by the numerals 1,2,...,n. All groups and sets will be understood to be finite, and sets are non-null unless otherwise specified. The order of a set M is the number of objects in the set and will be denoted as o(M).

Definition 1. A permutation of a set M is a one-to-one mapping of M onto M(6,1)[1].

If a set M contains n objects, o(M) = n, it can be written as $M = \{1,2,\ldots,n\}$, or as $M = \{a_1,a_2,\ldots,a_n\}$. For a permutation f, $(a_i)f = a_j$ means that a_j is the image of a_i under f; Mf = M. A permutation can be represented in various ways. One of the most elementary but very cumbersome is the two row form, where

$$f = \begin{pmatrix} 1 & 2 & \ldots m \\ a_1 & a_2 & \ldots a_m \end{pmatrix}$$

means that 1 is mapped onto the number a_1 under f, 2 onto $a_2,\ldots,m$ onto a_m. A more convenient notation arises when f is such that $(a_1)f = a_2$, $(a_2)f = a_3,\ldots,(a_{m-1})f = a_m$, $(a_m)f = a_1$. The symbol $(a_1a_2\ldots a_m)$, called an m-cycle, denotes this permutation and is referred to as cyclic notation. Note that $(a_1a_2\ldots a_m) = (a_2a_3\ldots a_ma_1) = (a_ma_1\ldots a_{m-1})$. It will be shown later that every permutation can be expressed by using cyclic notation. The degree

---

[1] The notation (6,1) refers to page 1 of reference number 6 in the bibliography. Similar notation is used throughout this report.

of a permutation is the number of distinct objects it maps onto objects other than themselves. Two permutations f and g are said to be equal if $(a_i)f = (a_i)g$ for all $a_i \varepsilon M$.

The "identical" permutation is the identity mapping e where $(a_i)e = a_i$ for all $a_i \varepsilon M$. The inverse of any permutation g, denoted by g^{-1}, is the one-to-one mapping such that if $(a_i)g = a_j$, then $(a_j)g^{-1} = a_i$. The product, or composition, of two permutations f and g is defined to be the one-to-one mapping fg obtained by first performing f and then g; that is, $(a)fg = (af)g$ for all $a \varepsilon M$. Thus, if $M = \{1,2,3,4,\}$,

$$f = \begin{pmatrix}1234\\2341\end{pmatrix},\ g = \begin{pmatrix}1234\\3124\end{pmatrix},\ \text{then } fg = \begin{pmatrix}1234\\1243\end{pmatrix},\ \text{but } gf = \begin{pmatrix}1234\\4231\end{pmatrix} \neq fg$$

which illustrates the fact that permutation multiplication is, in general, not commutative. It is associative, however.

The following well-known theorem is easily proved with the above definitions.

Theorem 1. For any set M with $n>1$ elements, the set of all permutations of M forms a group under permutation multiplication.

This particular group is called the symmetric group on M and will be denoted by Sym(M). Since there are n! permutations of n elements, o(Sym(M)) = n! and Sym(M) is said to be of degree n. The degree refers to the number of objects actually mapped by Sym(M); in this case Deg(Sym(M)) = n = o(M).

Now consider a permutation $f \varepsilon Sym(M)$. If $a,b \varepsilon M$, define $a \equiv_f b$ if and only if $b = (a)f^i$ for some integer i. This defines an equivalence relation on M.

1) For every $a \varepsilon M$, $a \equiv_f a$, since $a = (a)f^0 = (a)e = a$.

2) For $a,b \in M$, if $a \equiv_f b$, then $b = (a)f^i$ for some integer i so that $a = (b)f^{-i}$. Whence $b \equiv_f a$.

3) For $a,b,c \in M$, if $a \equiv_f b$, $b \equiv_f c$, then $b = (a)f^i$, $c = (b)f^j$ for some integers i and j. Then $c = ((a)f^i)f^j = (a)f^if^j = (a)f^{i+j}$. This implies $a \equiv_f c$.

This equivalence relation induces a decomposition of M into disjoint subsets, namely the equivalence classes. In particular, since M is finite, if $a \in M$ there is a smallest positive integer k such that $(a)f^k = a$. Then the equivalence class containing a consists of the elements a, $(a)f, \ldots, (a)f^{k-1}$, and f is the k-cycle $(a\ (a)f\ (a)f^2 \ldots (a)f^{k-1})$ on the elements in this equivalence class. Thus given any permutation f on a set M, M can be decomposed into equivalence classes and f is a cycle on each disjoint set. Then f can be represented as the product of these disjoint cycles, since the image of every element under f will be known. This representation is unique except for the order of the cycles and the alternate ways each cycle can be written. It is customary to omit the cycles of length one, it being understood that objects omitted are mapped onto themselves under the particular permutation. For example,

$$\begin{pmatrix} 12345 \\ 12453 \end{pmatrix} = (1)(2)(345) = (345).$$

When a permutation is a cycle, for example $f = (a_1a_2 \ldots a_m)$, the powers of f are easy to compute if the m objects are visualized as being arranged in a circle. In general, f^k maps each object a_i onto a_{i+k}, where i+k is reduced modulo m. Then f^m will map each object back onto itself, and thus the order of a cycle (in a group) is equal to its degree.

Lemma 1. The order of a permutation f is the least common multiple of the orders of its cycles.

Proof: Let f be a permutation and $f = g_1g_2\cdots g_m$ be the cyclic decomposition of f, where the order of g_i is u_i. If $a \varepsilon M$, a belongs to one of the cycles, say g_k, then $(a)g_k^{u_k} = a$. Also $(a)f^t = a$ if t is a multiple of u_k. Conversely, if $(a)f^t = a, a\varepsilon g_k$, then t must be a multiple of u_k. Then $(a_i)f^t = a_i$ for all $a_i \varepsilon M$ if and only if t is a multiple of each of the u_k, in which case $f^t = e$. The smallest such t is the order of f and this is the least common multiple of $\{u_1, u_2, \ldots, u_m\}$.

The simplest non-identical permutations are the 2-cycles, called transpositions. Every permutation is a product of transpositions since $(12\ldots n) = (12)(13)\ldots(1n)$, but this representation is not unique. However, the following well-known lemma pertains to representing a permutation as a product of transpositions (a_ia_j).

Lemma 2. In any representation of a permutation by transpositions, the number of transpositions is always even or always odd.

Definition 2. If a permutation is expressible as an even number of transpositions, it is called an even permutation. If it is expressible as an odd number, it is called an odd permutation.

The following facts follow immediately. A transposition is an odd permutation; the product of two even (or odd) permutations is even, while the product of an odd and an even (in either order) is an odd permutation, and the identity permutation is even, since e = (ab)(ba).

Theorem 2. The even permutations on a set M form a normal subgroup of index two in Sym(M)(2,59).

Proof: Let Alt(M) be the set of all even permutations on M and $f,g \varepsilon Alt(M)$. Then $fg \varepsilon Alt(M)$ since the product of two even permutations is even. Suppose $f^{-1} \notin Alt(M)$. Since $f \varepsilon Alt(M)$, ff^{-1} is odd and $ff^{-1} \notin Alt(M)$, but this a contradiction since $ff^{-1} = e \varepsilon Alt(M)$. Thus $f^{-1} \varepsilon Alt(M)$ for any $f \varepsilon Alt(M)$ and Alt(M) is a subgroup of Sym(M), called the alternating group. To show that Alt(M) is normal in Sym(M), let W be the group of real numbers 1 and -1 under multiplication. Define the mapping T of Sym(M) onto W by $(f)T = 1$ if f is an even permutation, $(f)T = -1$ if f is an odd permutation. By the rules for multiplication of even and odd permutations, T is a homomorphism of Sym(M) onto W. That is, if $f_1, f_2 \varepsilon Sym(M)$, $h_1, h_2 \varepsilon W$, and $(f_1)T = h_1$, $(f_2)T = h_2$, then $(f_1 f_2)T = h_1 h_2$. The kernel of T is precisely Alt(M), since every even permutation goes onto 1, and being the kernel of a homomorphism, Alt(M) is a normal subgroup of Sym(M). Now since $(a_1 a_2)$ is an odd permutation, the right coset $Alt(M)(a_1 a_2)$ consists entirely of odd permutations. If $f \varepsilon Sym(M)$, f is either even or odd; if even $f \varepsilon Alt(M)$; if odd $f(a_1 a_2)$ is even, $f(a_1 a_2) \varepsilon Alt(M)$ and $f = (f(a_1 a_2))(a_1 a_2) \varepsilon Alt(M)(a_1 a_2)$. Thus $Sym(M) = Alt(M) + Alt(M)(a_1 a_2)$ where the plus sign indicates the cosets Alt(M) and $Alt(M)(a_1 a_2)$ are distinct and exhaust the elements of Sym(M). Since there are two right cosets of Alt(M) in Sym(M), Alt(M) is of index two in Sym(M) and the theorem is proved.

The last part of the proof, that Alt(M) is of index two in Sym(M), is sufficient to prove that Alt(M) is a normal subgroup. If Alt(M) is of index two, then

$$2 = \frac{o(Sym(M))}{o(Alt(M))} = \frac{n!}{o(Alt(M)} \text{ so that } o(Alt(M)) = \frac{n!}{2}.$$

There are as many even permutations in Sym(M) as there are odd, since right cosets of Alt(M) contain the same number of elements. There are several interesting properties of alternating groups. These will be discussed later when stronger concepts are available.

CAYLEY'S THEOREM

When groups first arose in mathematics they usually came from some specific source and in some very concrete form. Very often it was in the form of a set of transformations of some particular mathematical object. In fact, most finite groups appeared as groups of permutations, that is, as subgroups of Sym(M). The English mathematician Cayley first noted that every group could be realized as a subgroup of Sym(M) for some M(3,60).

Theorem 3. Every group G is isomorphic to a permutation group of its own elements (2,9).

Proof: Let G be a group with k elements and identity element i. For each $g \varepsilon G$, define the mapping R(g): $(x)R(g) = xg$ for all $x \varepsilon G$. For a fixed g this is a mapping of the elements of G onto themselves, since for a given $y \varepsilon G$, $(yg^{-1})R(g) = yg^{-1}g = yi = y$. It is also one-to-one since if $x_1, x_2 \varepsilon G$ and $x_1 g = x_2 g$, then $x_1 = x_2$ by the cancellation law for groups. Thus R(g) is a permutation for each g and in the two row form

$$R(g) = \begin{pmatrix} x_1 & x_2 & \cdots x_k \\ x_1 g & x_2 g & \cdots x_k g \end{pmatrix}.$$

To show that G is isomorphic to $G^1 = \{R(g)|g\varepsilon G\}$, consider the following. The mapping $R(g_1)R(g_2)$ is the mapping $(x)R(g_1)R(g_2) = (xg_1)R(g_2) = (xg_1)g_2 = x(g_1g_2)$ for all $x\varepsilon G$ so $R(g_1)R(g_2) = R(g_1g_2)$. Moreover, $(i)R(g_1) = g_1$, $(i)R(g_2) = g_2$ so if $g_1 \neq g_2$, then $R(g_1) \neq R(g_2)$. Thus the mapping F, $(g)F = R(g)$, is an isomorphism of G onto G^1, a group of permutations, and the theorem is proved. Moreover, $R(i) = e$, and the inverse of $R(g)$ is $R(g^{-1})$ since $R(g^{-1})R(g) = R(g^{-1}g) = R(i) = e$ implies $(R(g))^{-1} = R(g^{-1})$.

A permutation is said to be regular if all of its cycles are of the same degree. Every permutation in G^1 is regular. If $R(g)\varepsilon G^1$, suppose the element g of the original group G is of order r, $g^r = i$. To resolve R(g) into cycles, let x_1 be any element of G. Then R(g) contains the cycle $(x_1x_1g\ldots x_1g^{r-1})$. If x_2 is any other element of G not in this cycle, form $(x_2x_2g\ldots x_2g^{r-1})$. This process can be continued until all elements of G have been accounted for. Thus $R(g) = (x_1x_1g\ldots x_1g^{r-1})(x_2x_2g\ldots x_2{}^{r-1})\ldots (x_mx_mg\ldots x_mg^{r-1})$ and every cycle is of the same degree so R(g) is regular. For this reason G^1 is called the right regular representation of G. It is also possible to consider the permutations L(g): $(x)L(g) = gx$ for all $x\varepsilon G$. The group of these permutations is called the left regular representation of G. L(g) is anti-isomorphic to G. It is one-to-one but "reverses" multiplication, that is, $L(g_1g_2) = L(g_2)L(g_2)$. Thus a group has more than one representation in terms of permutations; in fact, it can have representations of different degree. It is sometimes advantageous to keep the degree as small as possible; note that the right regular representation G^1 is a subgroup of Sym(G), where $o(G^1) = k$, $o(Sym(G)) = k!$ and G^1 is rather "lost" in Sym(G). It is possible to find smaller sets M such that

G will be isomorphic to a subgroup of Sym(M), but this is presented later. The main advantage of Cayley's theorem is that it enables one to represent a purely abstract group by a permutation group, as in the following example.

Example 1. Let G be the abstract non-Abelian group of order 6 defined by the following table (4,81).

.	i	a	b	c	d	f
i	i	a	b	c	d	f
a	a	b	i	f	c	d
b	b	i	a	d	f	c
c	c	d	f	i	a	b
d	d	f	c	b	i	a
f	f	c	d	a	b	i

Then the mappings R(i) = e, R(a) = (iab)(cdf), R(b) = (iba)(cfd), R(c) = (ic)(af)(bd), R(d) = (id)(ac)(bf), R(f) = (if)(ad)(bc) make up the group G^1 which is isomorphic to a subgroup of Sym ($\{1,2,3,4,5,6\}$). On the other hand G is also isomorphic to Sym ($\{1,2,3\}$) under the mapping E; (i)E = (1), (a)E = (123), (b)E = (132), (c)E = (12), (d)E = (13), (f)E = (23).

It will be shown later by using cosets, that some groups can be shown to be isomorphic to subgroups of Sym(M) for quite small o(M); however, no smaller o(M) can be obtained in the above example.

The following lemma is an application of Cayley's theorem for abstract groups (6,10).

Lemma 3. If o(G) = 2u with u odd, then G contains a normal subgroup of order u.

Proof: G contains an element g of order 2 by one of the Sylow theorems. From this it follows that R(g) is a product of u transpositions and is therefore an odd permutation. Hence G^1 contains odd permutations, and therefore the subgroup N^1 consisting of all the even permutations of G^1 is a normal subgroup of index 2. The desired normal subgroup of G is then the subgroup of G to which N^1 corresponds.

CONJUGATES IN A SYMMETRIC GROUP

The idea of conjugates is a very fundamental concept of elementary group theory. Conjugate permutations will be approached by first considering the idea of a partition.

Definition 3. Given the integer n, the sequence of positive integers $n_1, n_2, \ldots n_r$, $n_1 \leq n_2 \leq \ldots \leq n_r$ constitute a partition of n if $n = n_1 + n_2 + \ldots + n_r$ (3,75).

Let p(n) denote the number of partitions of n. As an example, p(4) = 5 since 4 = 4, 4 = 1 + 3, 4 = 1 + 1 + 2, 4 = 1 + 1 + 1 + 1, and 4 = 2 + 2. Every time a permutation in Sym(M) is written as a product of disjoint cycles, with 1-cycles included, a partition of n is obtained. A permutation $f \varepsilon Sym(M)$ is said to have the cycle decomposition $\{n_1 n_2 \ldots n_r\}$ if it can be written as the product of disjoint cycles of lengths $n_1, n_2 \ldots n_r$, $n_1 \leq n_2 \leq \ldots \leq n_r$. Thus when n = 9, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 5 & 6 & 4 & 7 & 9 & 8 \end{pmatrix} = (1)(23)(456)(7)(89)$ has cycle decomposition $\{1,1,2,2,3\}$ and 9 = 1 + 1 + 2 + 2 + 3.

It is often important to know how many permutations belong to a certain partition of n. The formula for the number of permutations is due to Cauchy (4,73). If p_j is the number of cycles of degree j corresponding to the partition $1p_1 + 2p_2 + \ldots + kp_k$, then the exact number of distinct permutations with the cycle decomposition corresponding to this partition is

$$\frac{n!}{\prod_{j=1}^{k} j^{p_j}\, p_j!}$$

It will be shown that this is the number of permutations in any conjugate class.

A simple rule for computing products such as $h^{-1}gh$ is necessary for the following discussion. Suppose that $g \varepsilon \mathrm{Sym}(M)$, and $(a_i)g = a_j$. For any $h \varepsilon \mathrm{Sym}(M)$, suppose $(a_i)h = b$, $(a_j)h = c$. Then $(b)h^{-1}gh = (bh^{-1})gh = (a_i)gh = (a_i g)h = (a_j)h = c$. Thus to write $h^{-1}gh$, one replaces every symbol in g by its image under h. This is illustrated when g and h have been decomposed into cycles. Suppose g = (123)(4)(6587) and h = (158)(47362). Then to write $h^{-1}gh$, in g replace 1 by its image under h, which is 5, 2 by 4, 3 by 6,... 7 by 3. Thus $h^{-1}gh$ = (546)(7)(2813).

<u>Theorem 4.</u> Two permutations $f, g \varepsilon \mathrm{Sym}(M)$ are conjugate in Sym(M) if and only if f and g have the same number of cycles of any order.

<u>Proof:</u> Suppose f and g have the same cycle decomposition $\{r,s,\ldots,t\}$. Let $g = (a_{11}\cdots a_{1r})(a_{21}\cdots a_{2s})\cdots(a_{m1}\cdots a_{mt})$ and $f = (b_{11}\cdots b_{1r})(b_{21}\cdots b_{2s})$ $\cdots(b_{m1}\cdots b_{mt})$. Then if

$$h = \begin{pmatrix} a_{11}\cdots a_{1r}a_{21}\cdots a_{2s}\cdots a_{m1}\cdots a_{mt} \\ b_{11}\cdots b_{1b}b_{21}\cdots b_{2s}\cdots b_{m1}\cdots b_{mt} \end{pmatrix},$$

$h \varepsilon \mathrm{Sym}(M)$, $h^{-1}gh = f$ by applying the rule above, and so f and g are conjugate. Now suppose f and g are two conjugate permutations, $f = h^{-1}gh$ for some $h \varepsilon \mathrm{Sym}(M)$. Then by the rule to compute $h^{-1}gh$, f and g have the same cycle decomposition.

All the elements conjugate to a given element g are said to belong to the conjugate class of g. The conjugate relation is an equivalence relation on the set of elements forming a group.

Lemma 4. The number of conjugate classes in Sym(M) is p(n).

Proof: Each partition of an integer n corresponds to a particular decomposition, and two permutations with the same cycle decomposition are conjugate.

The above discussion can be applied to find all the elements commuting with a given permutation. A fundamental theorem in group theory is that the number of elements conjugate to an element $g \varepsilon G$ is the index of the normalizer of g in G, $[G:N_{(g)}]$. Combining this fact with Cauchy's formula, one can determine the normalizer of a particular element.

Example 2. Given the permutation $(12) \varepsilon Sym(M)$, what permutations commute with it? Any of the $(n-2)!$ permutations which leave 1 and 2 fixed commute with (12), and it commutes with itself. All of the $2(n-2)!$ elements $(12)^i g$ for $i = 0$ or 1, g fixing 1 and 2 commute with (12); however, there might be more. The number of distinct transpositions in Sym(M) can be computed from Cauchy's formula. A transposition corresponds to the cycle decomposition with (n-2) 1-cycles and one 2-cycle. In Cauchy's formula,

$$\frac{n!}{1^{n-2}(n-2)!2^1 1!} = \frac{n(n-1)}{2}$$

is the number of distinct transpositions, or by Theorem 4, the number of conjugates of (12). Suppose $r = o(N_{(12)})$; then r is the number of elements commuting with (12). Hence

$$\frac{n(n-1)}{2} = \left[Sym(M):N_{(12)}\right] = \frac{o(Sym(M))}{o(N_{(12)})} = \frac{n!}{r}$$

and $r = 2(n-2)!$. This many elements have already been exhibited so the general element f commuting with (12) is $f = (12)^i g$, $i = 0,1$, g fixing 1 and 2.

As another application, consider the cycle $f = (12...h)\varepsilon Sym(M)$. It will be shown that f commutes only with its own powers. Certainly it does commute with the n powers f^i, $i = 1,2,...n$. Any n cycle is conjugate to f; by Cauchy's formula there are $(n-1)!$ distinct n-cycles in Sym(M). If $r = o(N_{(f)})$, $(n-1)! = \frac{n!}{r}$ and $r = n$. Then there are n elements commuting with f, precisely the n powers of f(3,76).

TRANSITIVITY

The concept of transitivity distinguishes permutation groups from abstract groups in that transitivity applies only to the former. In this section permutation groups other than symmetric groups will be considered. Every group is a subgroup of some symmetric group.

Theorem 5. Let G be a subgroup of Sym(M) and $S \subseteq M$. Then $G_S = \{f\varepsilon G: (b_i)f = b_i \text{ for every } b_i\varepsilon S\}$ is a subgroup of G and $H = \{f\varepsilon G: Sf = S\}$ is a subgroup such that G_S is normal in H(2,55).

Proof: Let $S = \{b_1,b_2,...b_m\}$. If $g_1\varepsilon G_S, g_2\varepsilon G_S$, then $(b_i)g_1g_2^{-1} = (b_ig_1)g_2^{-1} = (b_i)g_2^{-1} = (b_ig_2)g_2^{-1} = (b_i)g_2g_2^{-1} = (b_i)e = b_i$, and hence

G_S is a subgroup. If $h_1 \varepsilon H$, $h_2 \varepsilon H$, then $(S)h_1h_2^{-1} = (Sh_1)h_2^{-1} = (S)h_2^{-1}$ $(Sh_2)h_2^{-1} = (S)h_2h_2^{-1} = (S)e = S$, so H is a subgroup. If $h \varepsilon H$, $g \varepsilon G_S$, then $(b_i)h \varepsilon S$, $(b_i)g = b_i$, $h^{-1} \varepsilon H$, where $(b_i)h^{-1} = b_j$. Then $(b_j)h^{-1}gh = (b_jh^{-1})gh$ $= (b_j)gh = (b_jg)h = (b_j)h = b_i$, which implies $h^{-1}gh \varepsilon G_S$ and thus G_S is a normal subgroup of H.

A special case of the above theorem is obtained when $S = \{a_i\}$. Then $G_S = G_{a_i}$ is the set of permutations which fix the element a_i, and $G_{a_i} = G_S = H$ is a subgroup of G.

An orbit of $G \subseteq Sym(M)$ is a set $T \subseteq M$ such that there exists an $a \varepsilon M$ for which $T = aG$(5,255). The different orbits of G partition M.

Theorem 6. If $G \subseteq Sym(M)$, $a \varepsilon M$, $b \varepsilon M$, then

1. $b \varepsilon aG$ if and only if $bG = aG$.
2. M is the disjoint union of the orbits of G(5,255).

Proof: 1. If $b \varepsilon aG$, then $b = (a)g$ for some $g \varepsilon G$. Then $bg = (ag)G$ $= (a)gG = aG$. Let $bG = aG$. Then $b \varepsilon bG$ since $e \varepsilon G$ and $b = (b)e$. Since $bG = aG$, $b \varepsilon aG$. 2. If $c \varepsilon bG \cap aG$, then $c \varepsilon bG$, $c \varepsilon aG$, so $cG = bG = aG$ by 1. Hence unequal subsets are disjoint. Since for any $a_i \varepsilon M$, $a_i = (a_i)e \varepsilon a_iG$, M is the union of the pairwise disjoint orbits of G.

Definition 4. A permutation group $G \subseteq Sym(M)$ is said to be transitive if and only if it has only one orbit (namely M). Otherwise G is intransitive.

Thus $M = aG$ for all $a \varepsilon M$ if G is transitive. G cannot be the identity alone, since $M \neq (a)e$ if M contains more than one element. Also, if

$a,b \varepsilon M$, $aG = bG$, which implies $b \varepsilon aG$, $b = (a)g$ for some $g \varepsilon G$.

Definition 4a. A permutation group $G \subseteq Sym(M)$ is said to be transitive if for any $a,b \varepsilon M$, there exists a $g \varepsilon G$ such that $(a)g = b$.

The symmetric group is transitive, but the subgroup $G = \{(1), (12), (34), (12)(34)\}$ of Sym ($\{1,2,3,4\}$) has order and degree 4 and is intransitive, since $1G = \{1,2\} \neq \{1,2,3,4\}$. Equivalently, there is no $f \varepsilon G$ such that $(1)f = 3$. A group G may fail to be transitive, but will be transitive on a subset of M; in particular G will be transitive on each of its orbits.

Definition 5. A permutation group $G \subseteq Sym(M)$ is transitive on a subset $S \subseteq M$ if $(a_i)f \varepsilon S$ for all $f \varepsilon G$ and $a_i \varepsilon S$, and if $a,b \varepsilon S$, there exists a $f \varepsilon G$ such that $(a)f = b$. S is called a set of transitivity for G(2,55).

Orbits of G and sets of transitivity for G are related as follows.

Theorem 7. A set $S \subseteq M$ is a set of transitivity for $G \subseteq Sym(M)$ if and only if S is an orbit of G.

Proof: Let $S = aG$ be an orbit of G for some $a \varepsilon M$, and let $g \varepsilon G$, $b \varepsilon S$. Then there exists an $f \varepsilon G$ such that $(a)f = b$. If $(b)g = c$, then $c = (b)g = (af)g = (a)fg \varepsilon S$ since $fg \varepsilon G$. Let $c,d \varepsilon S$. Then there exists $f,g \varepsilon G$ such that $(a)f = c$, $(a)g = d$, $f^{-1} \varepsilon G$ so $(c)f^{-1}g = (a)g = d$, and S is a set of transitivity for G. If S is a set of transitivity for G it is an orbit of G, since $S = aG$ for all $a \varepsilon S$.

Theorem 8. In a transitive group $G \subseteq Sym(M)$, the normalizer of G_a is transitive on the points left fixed by G_a(6,7).

Proof: Let $N_{(G_a)} = \{g \varepsilon G: gG_a = G_a g \text{ (or } G_a = g^{-1}G_a g)\}$ and $S = \{a_i \varepsilon M: (a_i)g = a_i \text{ for all } g \varepsilon G_a\}$. Let $h \varepsilon N_{(G_a)}$ and $b \varepsilon S$; if $(b)h = c$, then $c = (b)h = (bG_a)h = (b)G_a h = (ch^{-1})G_a h = (c)h^{-1}G_a h = (c)G_a$ since $h \varepsilon N_{(G_a)}$. Thus $(c)G_a = c$ so $c \varepsilon S$. Let $b,c \varepsilon S$, and $a \varepsilon S$ by hypothesis. Since G is transitive, there exists an $h \varepsilon G$ such that $(b)h = a$. Form the group $V = h^{-1}G_a h$ which leaves a fixed, since if $g \varepsilon G_a$, then $(a)h^{-1}gh = (ah^{-1})gh = (b)gh = (bg)h = (b)n = a$. Then $V \subseteq G_a$ and V has the same number of elements as G_a so $V = G_a$. Thus $G_a = h^{-1}G_a h$ so $h \varepsilon N_{(G_a)}$. Similarly for c there exists a $g \varepsilon G$ such that $(c)g = a$ and $g \varepsilon N_{(G_a)}$. Then $(b)gh^{-1} = (bh)g^{-1} = (a)g^{-1} = c$ and $N_{(G_a)}$ is transitive on S.

The above theorem is attributed to Jordan and has been generalized by W. A. Manning(6,7). Groups $G_S \subseteq Sym(M)$ which are transitive on M-S possess the property that if G_S and G_T are two such groups, $o(T) \leq o(S)$, and if G is transitive on M, there exists a $g \varepsilon G$ such that $g^{-1}G_S g \subseteq G_T$.

The decomposition of a permutation group into cosets can be accomplished by using sets of transitivity.

Theorem 9. If $S \subseteq M$ is a set of transitivity for $G \subseteq Sym(M)$, $a_1 \varepsilon S$, $G_{a_1} \subseteq G$, then $G = G_{a_1}f_1 + G_{a_1}f_2 + \ldots + G_{a_1}f_m$, where for each $a_i \varepsilon S$, $(a_1)f_i = a_i$(2,55).

Proof: Suppose $h \varepsilon G_{a_1}f_k$ and $h \varepsilon G_{a_1}f_j$, $f_k \neq f_j$. Then $h = g_1 f_k$, $h = g_2 f_j$ for some $g_1, g_2 \varepsilon G_{a_1}$. Thus $(a_1)h = (a_1)g_1 f_k = (a_1 g_1)f_k = (a_1)f_k = a_k$ and $(a_1)h = (a_1)g_2 f_j = (a_1 g_2)f_j = (a_1)f_j = a_j$. Since $f_k \neq f_j$, $a_k \neq a_j$ which is impossible. Thus the cosets $G_{a_1}f_i$ are distinct. Moreover, let h be an arbitrary element of G. Then $(a_1)h = a_i$ for some $a_i \varepsilon S$ since S is a set of transitivity for G. Then $(a_1)hf_i^{-1} = (a_1h)f_i^{-1} = (a_i)f_i^{-1} = a_1$, so $hf_i^{-1} \varepsilon G_{a_1}$, $hf_i^{-1}f_i = he = h$, $h \varepsilon G_{a_1} f_i$, and so the cosets $G_{a_1} f_i$ exhaust G.

In the proof of the theorem, the following corollary was also proved, since the index of G_{a_1} in G, $[G:G_{a_1}]$, is the number of right cosets in G.

Corollary 9.1 If $S \subseteq M$ is a set of transitivity for $G \subseteq Sym(M)$ which contains exactly m letters, then G_{a_1} is of index m in G.

Corollary 9.1 also says that if $G \subseteq Sym(M)$ is a permutation group, T is an orbit of G and $a \varepsilon T$, then $o(G) = o(G_a)o(T)$ and if G is transitive $o(G) = o(G_a)Deg(G)$. The converse of Theorem 9 is true only when S = M.

Theorem 10. A group $G \subseteq Sym(M)$ is transitive on $M = \{a_1, a_2, \ldots, a_n\}$ if $[G:G_{a_i}] = n$ for any fixed a_i, $i = 1,2,\ldots n$.

Proof: Let $G = G_{a_i}g_1 + G_{a_i}g_2 + \ldots + G_{a_i}g_n$ and let $T = a_iG$. The theorem will be proved by showing T = M. No two of the permutations g_i, i = 1,2,.,n say g_m and g_k, map a_i onto the same object. To do so would imply $(a_i)g_kg_m^{-1} = a_i$, $g_kg_m^{-1}\ G_{a_1}$, and this implies $G_{a_i}g_k = G_{a_i}g_m$ which is impossible. Since there are n such permutations and n objects in M, the permutations g_j, $j = 1,2,\ldots,n$, map a_i onto each a_j M. Thus $T = a_iG = M$. M is the only orbit for G, since if $a_kG = S$ were another, $a_k \varepsilon S$, but $a_k \varepsilon M$ and by Theorem 6, M = S.

Definition 6. A permutation group G on M is called semiregular if for each $a \varepsilon M$, $G_a = \langle e \rangle$. G is called regular if it is semiregular and transitive (5,8).

Accordingly, every regular group is also semiregular, and subgroups of semiregular groups are semiregular.

Lemma 5. All orbits of a semiregular group G have the same length, namely o(G).

Proof: Let T be an orbit of a semiregular group G. By Corollary 9.1 $o(G) = o(G_a)o(T) = 1o(T) = o(T)$.

The order of a semiregular group G is a divisor of its degree, since if G operates on M, by Theorem 6 M is the union of the disjoint orbits, and by Lemma 5, each orbit has length of o(G).

Lemma 6. A transitive group is regular if and only if its order and degree are equal.

Proof: Let $G \leq Sym(M)$ be a transitive group such that $o(G) = o(M)$. If G is transitive, M is the only orbit of G, but by Corollary 9.1, $o(G) = o(G_a)o(M)$. Since $o(G) = o(M)$, $o(G_a)$ must be 1 and thus G is semiregular and consequently regular. Suppose G is a regular group. M is the only orbit of G and by Lemma 5, $o(G) = o(M)$.

Abelian groups have an interesting property concerning transitivity.

Theorem 11. Every transitive Abelian group is regular (5,265).

Proof: Suppose G is a transitive Abelian group that is not regular. Then G is not semiregular, so there exists a $g \in G$, $g \neq e$, and $a \in M$ such that $(a)g = a$. Since $g \neq e$, there is also some $b \in M$ such that $(b)g \neq b$. Since

G is transitive, there is some $h \in G$ such that $(a)h = b$. Then $(a)gh = (ag)h = (a)h = b$, and $(a)hg = (ah)g = (b)g \neq b$. Thus $gh \neq hg$, which contradicts the fact that G is Abelian. Thus every transitive Abelian group is regular.

An example will illustrate that every permutation in a regular permutation group is regular. If $f = (123)(45) \in Sym(\{1,2,3,4,5\})$ is a non-regular permutation, $f^2 = (132)(4)(5) \neq e$ maps 4 and 5 onto themselves, which contradicts the fact that in a regular permutation group, only the identity maps any object onto itself. The cyclic group $G = \langle (123)(456) \rangle = \{e, (123)(456), (132)(465)\} \subset Sym(\{1,2,3,4,5,6\})$ is an example of a group which is not regular because its order is not equal to its degree, although every permutation in it is regular. However, G is intransitive, since there is no $g \in G$ such that $(1)g = 4$. Regular permutation groups have an important application in the representation of groups as permutation groups. In fact, every group is isomorphic to a regular permutation group, since the permutation group G^1, the right regular representation of Theorem 3, is a regular permutation group. It is semi-regular, since only the identity R(i) fixes any object, and it is transitive since $G = aG^1$. Regular permutation groups are their own regular representations, and a transitive permutation group consisting of regular permutations only is a regular permutation group.

PERMUTATION REPRESENTATIONS

It has been noted that an abstract group may be represented in more than one way as a permutation group. A group of permutations P is called a representation of a group G if there is a mapping F of G onto P, (g)F = K(g), $g \varepsilon G$, $K(g) \varepsilon P$ such that $K(g_1)K(g_2) = K(g_1 g_2)$. P is necessarily a homomorphic image of G, and if P is, in fact, isomorphic to G, P is said to be a faithful representation of G. Just as all homomorphic images of G are given by factor groups modulo a normal subgroup of G, all transitive permutation representations of G may be found in terms of right cosets of subgroups (2,56).

It was noted in Example 1 that the non-Abelian group of order 6 could be faithfully represented as a transitive permutation group on three objects, and also on six objects. For this reason it is necessary to distinguish as permutation groups certain groups which are isomorphic as abstract groups.

<u>Definition 7.</u> A permutation group Q on a set S is isomorphic as a permutation group to a permutation group P on a set T if there is an isomorphism F between Q and P and a one-to-one correspondence E between S and T, $((s_i)E = t_i)$, such that $(s_i)q = s_j$ if and only if $(t_i)p = t_j$ when qF = p.

<u>Theorem 12.</u> If G is a group, H a subgroup of G and $S = \{Hg : g \varepsilon G\}$ then there is a homomorphism D of G into Sym(S), $GD = P^1 \subseteq \text{Sym}(S)$, such that P^1 is a representation of G as a transitive permutation group (2,57).

<u>Proof:</u> Let G be a group, H a subgroup of G, and $S = \{Hg : g \varepsilon G\}$. S need not be a group itself; in fact, it would be a group only if H were a normal subgroup of G. For $g \varepsilon F$, let the mapping Cg be defined by $(Hx)C_g = Hxg$ for every $g \varepsilon G$ and every $x \varepsilon G$. To show $C_g \varepsilon \text{Sym}(S)$, suppose $Hx \varepsilon S$. Then $Hx = (Hx)g^{-1}g = (Hxg^{-1})g = (Hxg^{-1})C_g$ so that C_g maps S onto itself. Moreover, C_g is

one-to-one, for if Hx, HyεS and $(Hx)C_g = (Hy)C_g$, then Hxg = Hyg, which by the cancellation property of groups implies that Hx = Hy. Thus for every gεG, $C_g \varepsilon Sym(S)$. If g,hεG, consider C_{gh}. For any HxεS, $(Hx)C_{gh} = Hxgh = (Hxg)h = (Hxg)C_h = (HxC_g)C_h = (Hx)C_gC_h$, and hence $C_{gh} = C_gC_h$. Thus the mapping D defined by $(g)D = C_g$ is a homomorphism of G into Sym(S), and is a representation for G. P^1 is a transitive representation of G since $(H)C_g = Hg$ is an arbitrary element of S, and it is sufficient for transitivity to show that a particular object can be mapped onto any other object. The degree of P^1 is $o(S) = [G:H]$.

Now, the question is, when is this representation faithful?

<u>Theorem 13.</u> The kernel of D in Theorem 12 is the largest normal subgroup of G which is contained in H. The representation is faithful if and only if H contains no normal subgroup of G greater than the identity (2,58).

<u>Proof:</u> Let K be the kernel of D. If kεK, then $(k)D = C_k$ is the identity map e on S, so that for every HxεS, $(Hx)C_k = Hxk = Hx$ for every xεG. On the other hand, if bεG is such that Hxb = Hx for every xεG, retracing the above argument bεK. Thus $K = \{b \varepsilon G\text{: } Hxb = Hx \text{ for all } x \varepsilon G\}$. K is a normal subgroup of G because it is the kernel of a homomorphism. Now $K \subseteq H$, for if kεK, Hxk = Hx for every xεG, so in particular Hk = H, hence kεH. Finally, let N be a normal subgroup of G which is contained in H. If yεN, xεG, then $xyx^{-1} \varepsilon N \subseteq H$ so that $Hxyx^{-1} = H$; thus Hxy = Hx for all xεG and so yεK. Thus the first half of the theorem follows. By the definition of faithful representations, and by the fact that a homomorphism is an isomorphism if and only if the kernel is the identity, the second statement

follows.

The case $H = \langle i \rangle$, i the identity element of G, yields Cayley's theorem, Theorem 3. If H has no normal subgroup of G in it other than $\langle i \rangle$, and $H \neq G$, then the size of M used in proving Theorem 3 has been decreased. This observation is useful both as a means of proving certain finite groups have nontrivial subgroups, and as a means of representing certain groups as permutation groups on small sets. Theorem 14 states that every transitive representation of a group is isomorphic to one of the type obtained in Theorem 12.

Theorem 14. Suppose GF = P is a representation of G as a transitive permutation group on a set of elements S.

1. If s is a particular element of S, then $H = \{g \varepsilon G : (s)f_g = s \text{ where } (g)F = f_g \varepsilon P\}$ is a subgroup of G.

2. The elements of S may be put into a one-to-one correspondence with the right cosets of H so that P is isomorphic as a permutation group to the group of permutations P^1 given in Theorem 12(2,57).

Proof: 1. If $g,h \varepsilon H$ then $(s)f_g = s$, $(s)f_h = s$ and $(s)f_{gh^{-1}} = (s)f_g f_{h^{-1}} = (sf_g)f_{h^{-1}} = (s)f_{h^{-1}} = (sf_h)f_{h^{-1}} = (s)f_{hh^{-1}} = (s)f_e = s$. Hence H is a subgroup. 2. $T = \{g \varepsilon G : (s)f_g = s_i \text{ for some fixed } s_i \varepsilon S\}$ is not vacuous since P is transitive. If x_i is one of the elements of T, then T is the right coset Hx_i, H being the subgroup found in 1. which fixes s, since if $g \varepsilon T$ then $(s)f_g = s_i$ so $g = eg \varepsilon Hx_i$. Conversely all the elements of a right coset Hx_j have the property that their corresponding permutations all map s onto the same element $s_j = (s)x_j$. This establishes a one-to-one correspondence between elements of S and right cosets of H. Let P^1 be the permutation group of right cosets found in Theorem 12, where $C_g \varepsilon P^1$ for every $g \varepsilon G$. In P if $(s_i)f_g = s_j$, then $(s)f_{x_i}f_g = (sf_{x_i})f_g = (s_i)f_g = s_j$, whence $x_i g \varepsilon Hx_j$, and hence $Hx_i g = Hx_j$. Conversely, $Hx_i g = Hx_j$ implies $(s_i)f_g = s_j$. Thus $(s_i)f_g = s_j$ if and only if $(Hx_i)C_g = Hx_j$. In particular, f_g is the identity if and only if C_g is the identity. Thus P and P^1 are homomorphic images of G, both with the same kernel, and K, where $f_g K = C_g$, is an isomorphism between P and P^1. With the one-to-one correspondence between S and the set of right cosets of H, it has been established that P is isomorphic as a permutation group to P^1.

Thus any transitive permutation representation of a group G may be spoken of as the representation on a subgroup H. The following lemma follows from the fact that the only subgroups of an Abelian group are normal and by Theorems 13 and 14.

Lemma 7. The only faithful transitive representation of an Abelian group is the regular representation.

PRIMITIVE AND IMPRIMITIVE GROUPS

Let G be a permutation group on a set M.

Definition 8. A block of G is a subset $B \subseteq M$ such that, if $g \varepsilon G$, either $B = Bg$ or $B \cap Bg = \emptyset$.

Obviously, the whole set, the empty set and every singleton are blocks. These are called trivial blocks. Also, if $H \subseteq G$, then every block of G is a block of H, and an orbit is a block.

Lemma 8. If B and D are blocks of G, then their intersection $B \cap D$ is also a block of G(6,12).

Proof: Let $C = B \cap D$. If $C \cap Cg = \emptyset$, there is nothing to prove. Suppose $a \in C \cap Cg$ for some $g \in G$. Then $a \in C$ which implies $a \in B$, $a \in D$, and $a \in Cg$ which implies that there exists a $b \in C$ such that $(b)g = a$. If $b \in C$, then $b \in B$ and $b \in D$; so $a \in Dg$ and $a \in Bg$. Hence when $C \cap Cg$ is non-empty, $B \cap Bg$ and $D \cap Dg$ are also non-empty. Since B and D are blocks, $B = Bg$, $D = Dg$. Hence $Cg = (B \cap D)g = Bg \cap Dg = B \cap D = C$, and so C is a block.

Lemma 9. If B is a block and $g \in G$, then Bg is a block (5,269).

Proof: Let $h \in G$. If $Bghg^{-1} = B$, then $Bg = Bghg^{-1}g = Bgh = (Bg)h$. If $Bghg^{-1} \cap B = \emptyset$, then $(Bg)h \cap Bg = \left[(Bg)h \cap Bg\right] g^{-1}g = \left[Bghg^{-1} \cap Bgg^{-1}\right]g = \left[Bghg^{-1} \cap B\right]g = \emptyset g = \emptyset$. Hence Bg is a block.

Theorem 15. If $B \neq \emptyset$ is a block for the transitive permutation group G, then the order of B divides the degree of G.

Proof: If $a \in M$, $b \in B$, then since G is transitive there exists a $h \in G$ such that $(a)h = b$, $(b)h^{-1} = a$ so $a \in Bg$ for $g = h^{-1}$. If B is a block, Bg is a block for each $g \in G$, B and Bg are of the same order and either disjoint or equal. Thus M is the disjoint union of all the Bg, and hence $o(B) | o(M)$.

Definition 9. A primitive permutation group is a transitive permutation group with no nontrivial blocks. An imprimitive permutation group is a transitive permutation group with at least one nontrivial block,

A block for an imprimitive group is often referred to as a set of imprimitivity. A block system of an imprimitive group G is a set S of nontrivial blocks such that $M = B_1 + B_2 + \ldots + B_k$, $B_i \varepsilon S$, and such that if $B \varepsilon S$ and $g \varepsilon G$, then $Bg \varepsilon S$(5,269).

<u>Theorem 16.</u> Let G be an imprimitive permutation group. If B is a nontrivial block then the set of distinct Bg, $g \varepsilon G$, is a block system. Conversely, any block system is of this type (5,269).

<u>Proof:</u> Let B be a nontrivial block and let $S = \{Bg : g \varepsilon G\}$. Since G is imprimitive, it is transitive, and therefore each $a \varepsilon M$ is in some Bg. If $Bg \cap Bh \neq \emptyset$, then $Bgh^{-1} \cap B \neq \emptyset$, and since B is a block, $Bgh^{-1} = B$, $Bg = Bh$. Hence M is the union of the disjoint blocks of S. Moreover, if $Bg \varepsilon S$ and $h \varepsilon G$, then $(Bg)h = B(gh) \varepsilon S$. Hence S is a block system. Conversely, let S be a block system and let $B \varepsilon S$. Then by definition $Bg \varepsilon S$ for all $g \varepsilon G$. Since the set of Bg, $g \varepsilon G$, is already a block system by the first half of the proof, and since M is the disjoint union of blocks of S it follows that $S = \{Bg : g \varepsilon G\}$.

<u>Theorem 17.</u> If G is an imprimitive group with block system S and $N = \{h \varepsilon G : Bh = B \text{ for all } B \varepsilon S\}$ then N is a normal intransitive subgroup of G(5,271).

<u>Proof:</u> N is a subgroup of G, since if $h, f \varepsilon N$, then $B(hf^{-1}) = (Bh)f^{-1} = (B)f^{-1} = (Bf)f^{-1} = B(ff^{-1}) = Bi = B$. If $g \varepsilon G$, $h \varepsilon N$ and $B \varepsilon S$, then $Bg^{-1} \varepsilon S$, so that $Bg^{-1}hg = (Bg^{-1})hg = (Bg^{-1})g = Bg^{-1}g = Bi = B$ and $g^{-1}hg \varepsilon N$. Thus N is a normal subgroup of G. Now, if $b \varepsilon B \varepsilon S$, then $B \neq M$ since S is a block system, and the orbit bN of N is a subset of B, hence a proper subset of M. Therefore N is intransitive.

Theorem 17 has a partial converse.

<u>Theorem 18.</u> If the transitive group G contains an intransitive normal subgroup N $\neq \langle i \rangle$, then G is imprimitive. The distinct orbits of N form a block system of G(6,13).

<u>Proof:</u> Let T be an orbit of N. Then Tg = aNg = agN = bN, so Tg is an orbit of N. Thus G can only permute the pairwise disjoint orbits of N among each other and hence the orbits of N form blocks of G. Because N $\neq \langle i \rangle$, they contain more than one object, and because of the intransitivity of N they are proper subsets of M. Hence G is a transitive permutation group with nontrivial blocks and is imprimitive. By Theorem 16, the set of distinct orbits form a block system of G.

The above theorem established a sufficient condition for imprimitivity; the following is a necessary and sufficient condition.

<u>Theorem 19.</u> Let aεM. The transitive group G on M is imprimitive if and only if there is a subgroup H which lies properly between G_a and G; i.e. for which $G_a \subset H \subset G$ holds (6,14).

<u>Proof:</u> Let G be imprimitive and B a nontrivial block of G. Let $H = \{h \varepsilon G\colon Bh = B\}$. In the proof of Theorem 17, H was shown to be a subgroup of G. H is a proper subgroup because $B \subset M$ and G is transitive. Let aεB, gεG_a. Because B is a block (B = Bg or $B \cap Bg = \emptyset$) it follows from (a)g = a that Bg = B. Therefore $G_a \subseteq H$. Because o(B)>1, there exists bεB, b $\neq$ a, and because of the transitivity of G there exists an fεG such that (a)f = b. Again, because B is a block Bf = B, fεH but $f \notin G_a$. Hence $G_a \subset H$. Now suppose H is given with $G_a \subset H \subset G$. Let B = aH. To show B is a block, let $b \varepsilon B \cap Bg$ with gεG. Then bεB, bεBg, hence b = (a)h = (a)fg where h,fεH. Then

$a = (a)hh^{-1} = (a)fgh^{-1}$ so $fgh^{-1} \varepsilon G_a \subset H$ and $g \varepsilon H$. Thus $Bg = (a)Hg = (a)H = B$ and B is a block. Because $G_a \subset H$, B does not consist of a alone. It has been shown that $B = Bg$ holds only for $g \varepsilon H$. Since $H \subset G$, there is a $g \varepsilon G$ with $B \neq Bg$, and therefore $B \neq M$. Hence B is a nontrivial block and G is imprimitive.

The above theorem can be applied in the following manner.

Theorem 20. Let G be a regular group on M whose degree is not a prime. Then G is imprimitive (6,15).

Proof: If G is regular, G is transitive and $G_a = \{e\}$. If o(M) is not a prime, by Corollary 9.1 o(G) is not a prime. Hence for $a \varepsilon M$ there is a proper subgroup between $G_a = \{e\}$ and G. By Theorem 19, G is imprimitive.

$G = \langle(1234)\rangle$ contains the elements e, (1234), (13)(24), (1432) and is imprimitive, having the nontrivial block $\{1,3\}$. The group $H = \{e, (12)(34), (13)(24), (14)(23)\}$ has 3 non-trivial blocks, $\{1,2\}$, $\{1,3\}$, $\{1,4\}$ and thus is imprimitive.

Several of the theorems on imprimitive groups have implications pertinent to primitive groups. In particular, the following theorems follow from Theorem 15, Theorem 19 and Theorem 18, respectively.

Theorem 21. If G is a transitive group on M whose degree is a prime, then G is primitive.

Proof: Let B be a block of G. Then by Theorem 15, o(B) divides o(M) = p. Hence o(B) is 1 or p and B is trivial in either case. Hence G is primitive.

Theorem 22. Let $a \epsilon M$ and $o(M) > 1$. A transitive group G on M is primitive if and only if G_a is a maximal subgroup of G.

Theorem 23. A normal subgroup $N \neq \langle e \rangle$ of a primitive group is transitive.

Primitive groups have some interesting properties of their own.

Theorem 24. If G is primitive on M and $a, b \epsilon M$, $a \neq b$, then either $G_a \neq G_b$ or G is a regular group of prime degree (6,17).

Proof: Let $G_a \neq \langle e \rangle$. Let P be the set of points of M which are left fixed by every permutation of G_a. By Theorem 8, $N(G_a) = N$ is transitive on P. If $G_a = G_b$ for $a \neq b$, then $b \epsilon P$ and there exists an $h \epsilon N$ such that $(a)h = b$, $h \notin G_a$ so $G_a \subset N$. By the assumed primitivity of G and by Theorem 22, $N = G$. Hence it follows that $P = M$ and $G_a = \langle e \rangle$ in contradiction to the assumption that $G_a \neq \langle e \rangle$. Thus $G_a \neq G_b$. If $G_a = \langle e \rangle$, then G is regular and hence $n = o(M)$ is by Theorem 20 a prime.

Primitive groups of prime degree are easy to construct. $G = \langle (12345) \rangle$ is of degree 5 and is transitive since $1G = \{1,2,3,4,5\}$. Hence by Theorem 21, G is primitive. The permutations (12354), (12453), (12435), (13452), (13245) also generate primitive permutation groups.

"In conclusion, it should be pointed out that to each transitive group G on M there are certain primitive groups (in general of smaller degree) which are called primitive components of G," (6,18). By inducing transitive groups on block systems which are homomorphic to G, a series of primitive components is obtained.

MULTIPLY TRANSITIVE GROUPS

There is a generalization to the concept of transitivity.

Definition 10. A permutation group G on a set M of order n is called k-ply (or k-fold) transitive if for every two ordered k-tuples $a_1a_2 \ldots a_k$ and $b_1b_2 \ldots b_k$ of objects of M(with $a_i \neq a_j$, $b_i \neq b_j$ for $i \neq j$) there exists a $g \in G$ such that $(a_i)g = b_i$, $i = 1,2,\ldots k$(6,19).

The transitivity discussed before is the same as 1-ply transitivity. Every k-ply transitive group is automatically j-ply transitive, where $j<k$. Sym(M) is k-ply transitive for $k \leq n$, and if a group is n-ply transitive for some n, it must be the symmetric group. If $k = 2$, the term doubly transitive is employed; for $k \geq 2$, the term is multiply transitive. A group which is transitive, but not doubly transitive, is called singly transitive or simply transitive. If a group is k-ply transitive but not (k+1)-ply transitive, k is said to be the degree of transitivity of the group. There is no transitive group of degree n whose degree of transitivity is n-1. Every group having a k-ply transitive group as a subgroup is itself k-ply transitive. Multiply transitive is a strong form of primitivity.

Theorem 25. Every doubly transitive group G is primitive.

Proof: Let G be a doubly transitive group $B \subset M$, $o(B)>1$. Then there exists $a,b \in B$, $a \neq b$, and a $c \in M-B$. Since G is 2-ply transitive, there exists a $g \in G$ such that $(a)g = a$, $(b)g = c$. Thus $a \in Bg \cap B$ so that $Bg \cap B \neq \emptyset$. Since $c \in Bg - B$, $Bg \neq B$. Therefore B is not a nontrivial block and G is primitive.

Theorem 26. Let G be transitive on M and $a \in M$. Then G is (k+1)-ply transitive on M if and only if G_a is k-ply transitive on $M-\{a\}$(6,19).

Proof: Suppose G_a is k-ply transitive on $M-\{a\}$. To show k-ply transitivity it is sufficient to show that a particular ordered k-tuple can be mapped into any other ordered k-tuple. Consider the ordered (k+1)-tuple $a, a_1 a_2 \ldots a_k$ and let $b, b_1 b_2 \ldots b_k$ be any other ordered k-tuple. Since G is transitive, there exists a $g \varepsilon G$ such that $(b)g = a$. If $(b_i)g = c_i$, $i = 1,2,\ldots k$, then there exists an $h \varepsilon G_a$ such that $(a)h = a$ and $(c_i)h = a_i$, $i = 1,2,\ldots k$, since G_a is k-ply transitive. Then $gh \varepsilon G$ and $(b_i)gh = a_i$, $i = 1,2,\ldots k$, $(b)gh = (a)h = a$. Thus G is (k+1)-ply transitive on M. Suppose G is (k+1)-ply transitive on M. Let $M = \{a_1, a_2, \ldots, a_n\}$ and $a = a_1$. G contains an element g such that $(a)g = a$, $(a_i)g = b_i$, $i = 2,3,\ldots k+1$ where $b_2 b_3 \ldots b_{k+1}$ is any ordered k-tuple and $a \neq b_i$ for any i. Then $g \varepsilon G_a$ and G_a is k-ply transitive on $M-\{a\}$.

As an example, $G = \mathrm{Alt}(\{1,2,3,4\})$ is doubly transitive, since $G_1 = \{e, (234), (243)\}$ is simply transitive on $M-\{1\}$. The proof of the following theorem is analogous to that of Theorem 26.

Theorem 27. Let G be transitive on M and $S \subset M$. If G is k-ply transitive on M and $o(S) = d<k$, then G_S is (k-d)-ply transitive on $M - S$.

Many of the theorems on transitivity can be generalized without difficulty to multiply transitive groups. In particular, Corollary 9.1 can be generalized.

Theorem 28. The order of a k-ply transitive group of degree n is divisible by $n(n-1)\ldots(n-k+1)$. The quotient is the order of any subgroup of the form G_S with $o(S) = k$(6,20).

The alternating group has several interesting properties concerning multiple transitivity.

Theorem 29. Alt(M) is (n-2)-ply transitive ($n \geq 3$) where o(M) = n(2,60).

Proof: Let $b_1 b_2 \ldots b_n$ be an arbitrary ordering of M. If

$$f = \begin{pmatrix} a_1 \ldots a_{n-2} a_{n-1} a_n \\ b_1 \ldots b_{n-2} b_{n-1} b_n \end{pmatrix} \text{ and } g = \begin{pmatrix} a_1 \ldots a_{n-2} a_{n-1} a_n \\ b_1 \ldots b_{n-2} b_{n-1} b_n \end{pmatrix} \text{ then } g = f(b_{n-1} b_n)$$

and so either f or g is even, the other odd. Hence one belongs to Alt(M) which implies Alt(M) is (n-2)-ply transitive. Because Alt(M) is of degree n, it is not (n-1)-ply transitive since this would imply n-ply transitive.

The alternating group can be shown to be simple, (contains no proper normal subgroup) except for n = 4, by using multiple transitivity properties (3,61).

The concept of k-ply transitivity may be strengthened or weakened in many ways. The most important is called sharp k-ply transitivity. A group G is called sharply k-ply transitive if, for any two ordered k-tuples of the type described previously, there is exactly one $g \varepsilon G$ which maps the first into the second. The sharply simple transitive groups are the regular groups and have no special structure, since every abstract group can be faithfully represented as a regular permutation group (6,23). Two other strengthening properties are those of k-ply primitive and half-transitive. A group G on M is k-ply primitive if it is k-ply transitive and the subgroups which leave k-1 points fixed are not only transitive on the rest but even primitive. A group G on M is called half-transitive if its orbits all have equal length >1(6,23).

A weakening of the concept of k-ply transitivity in which unordered k-tuples are used in place of ordered k-tuples is of importance for game theory (6,23). This is called s set-transitive.

<u>Definition 11.</u> A group G on M is s set-transitive ($1 \leq s \leq n-1$) if for every pair of subsets of M, S and T, each containing s elements, there exists a $g \in G$ such that $(S)g = T$(1,36).

From the definition, 1 set-transitive and transitive are the same thing, and if G is k-ply transitive, then G is s set-transitive for all $s \leq k$. With $M = \{1,2,3,4,5,6,7\}$, the group $G = \langle (1234567), (235)(476) \rangle$ is an example of a group which is 2 set-transitive but not doubly transitive. G is not 3 or 4 set-transitive. A group G of degree n is said to be set transitive if G is s set-transitive for all s, $1 \leq s \leq n-1$. The alternating group is set-transitive except for n = 2, and the symmetric group is set-transitive. Beaumont and Peterson proved that groups which are s set-transitive for at least one s are transitive, and if for at least one s>1, they are primitive. The values of n for which set-transitive groups other than the symmetric or alternating groups may exist have been found to be only 5,6,9, and only four such groups exist other than their conjugates, the alternating groups and the symmetric groups(1,40).

Many, but not all, non-Abelian simple groups can be represented as doubly transitive permutation groups. A counter-example of order $2^6 3^4 5$ has been pointed out by Parker(6,21).

Whereas there are numerous nontrivial doubly and triply transitive groups (Sym(M) and Alt(M) are considered to be trivial in this case) only two nontrivial quadruply transitive groups and two nontrivial quintuply transitive groups are known; they were found in 1861 by Matthieu. Their degrees are 11, 23, 17, 24 respectively. Structure and representation of these groups are of great interest in regard to simple groups(6,21).

For $k>6$, it is not known if there are nontrivial k-ply transitive groups; however, there are many estimates on the limit of transitivity of groups of degree n, with $k<3 \log n$ being one(6,21).

REFERENCES

1) Beaumont, R. A., and R. P. Peterson. "Set-Transitive Permutation Groups". Canadian Journal of Mathematics, 1955, 7:35-42.

2) Hall, Marshall Jr. The Theory of Groups. New York: The Macmillan Co., 1959.

3) Herstein, I. N. Topics in Algebra. New York: Blaisdell Publishing Company, 1964.

4) Ledermann, W. Introduction to the Theory of Finite Groups. New York: Interscience Publishers, Inc., 1957.

5) Scott, W. R. Group Theory. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1964.

6) Wielandt, Helmut. Finite Permutation Groups. Translated by R. Bercov. New York and London: Academic Press, 1964.

ACKNOWLEDGMENT

The writer wishes to express his appreciation to Dr. Robert D. Bechtel for his assistance in the preparation of this report.

SOME ELEMENTARY CONCEPTS OF PERMUTATION GROUPS

by

WILLIAM V. MADDEN

B. S., South Dakota State College, 1963

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1965

Some of the elementary concepts of permutation groups are considered in this report. A knowledge of elementary group theory is assumed throughout.

A permutation is a one-to-one mapping of a set M onto itself. Only finite sets are considered. A permutation can be represented in two row form, and it can also be expressed as a product of disjoint cycles. It is shown that in a group, the order of a permutation is the least common multiple of the order of the disjoint cycles in this expression. Permutations are called even or odd, depending on whether they are expressable as an even or odd number of 2-cycles.

It is well-known that for a set M, all the permutations of M form a group, the symmetric group. The alternating group, the set of all even permutations of the set M, is a normal subgroup of index two in the symmetric group. Cayley's theorem states that every abstract group is isomorphic to a permutation group, where the objects permuted are the elements of the original group. Conjugate permutations are approached by considering the partition of an integer which corresponds to a cycle decomposition or representation for a permutation. Two permutations in the symmetric group are conjugate if and only if when expressed as a product of cycles, each permutation has the same number of cycles of any order. The number of conjugate classes in the symmetric group is p(n), the partition of the number of objects in the set M.

The concept of transitivity is defined for permutation groups. Subgroups of the symmetric group on M are considered in the section on transitivity, especially subgroups which map particular objects, or sets of objects, onto themselves. A permutation group on M is transitive if for two arbitrary elements of M, the group contains a permutation that maps one object onto the other. A group can be transitive on the whole set M or on subsets of M which are called sets of transitivity. Permutation groups can be decomposed into cosets by employing sets of transitivity. Regular groups are transitive permutation groups in which only the identity maps any element onto itself. An important theorem in this section is that a transitive group is regular if and only if its order is equal to its degree. The degree of a group is the number of objects it maps onto objects other than themselves.

In addition to Cayley's theorem, there is another way to represent an abstract group. Given a group G with a subgroup H, let S be the set of all right cosets for H. Then there is a homomorphism of G into the symmetric group on S such that the image of G is a transitive permutation group. Conversely, any transitive representation of a group G is isomorphic as a permutation group to a permutation group on the set of cosets for some subgroup H.

From the idea of transitivity, the concepts of imprimitive and primitive groups are derived. Special subsets of M, called blocks, are defined for this purpose. If a transitive permutation group G on a set M has a block which is not M and which contains more than one object, then G is said to be imprimitive; otherwise G is primitive. A necessary and sufficient condition that the transitive permutation group G on M is imprimitive is that G has a proper subgroup H which lies between G and a subgroup of G which maps some object of M onto itself. Transitive groups on sets with a prime number of elements are primitive.

Transitive permutation groups are generalized to multiply transitive, or k-ply transitive groups. Instead of mapping a single element onto any other single element, a k-ply transitive group is concerned with mapping ordered k-tuples onto other ordered k-tuples. If $k \geq 2$, k-ply transitive groups are primitive. Several means of strengthening or weakening the idea of k-ply transitivity are mentioned in the final section of the report.