JOURNAL OF RESEARCH of the National Bureau of Standards — B. Mathematical Sciences
Volume 76B, Nos. 1 and 2, January-June 1972

Abstract Groups as Doubly Transitive Permutation Groups *

Russell Merris **

(December 12, 1971)

The question considered is this: Which abstract groups have representations as doubly transitive permutation groups? Moreover, given an abstract group, can all doubly transitive representations be found? The paper is expository. Various results which bear on the question are presented in an elementary way.

Key words: Character; cosets; matrix representation; nilpotent group; normalizer; solvable group.

1. Introduction

For a positive integer, n, let S_n denote the group of all permutations on $\{1,2,\ldots,n\}$. When $n=4$, we mean by (1 2 3) the permutation which sends 1 to 2, 2 to 3, 3 to 1, and 4 to 4. The symbol e will be used to denote the identity element of any group.

Let $G=\{e, (12), (34), (12)\,(34)\}$ and $H=\{e, (12)\,(34), (13)\,(24), (14)\,(23)\}$. Then G and H are isomorphic subgroups of S_4. But, as a group of functions on $\{1, 2, 3, 4\}$, H acts transitively while G does not.

This simple example shows that transitivity, like most of the interesting properties associated with permutation groups, is not a group theoretic property; it is not preserved under group isomorphism. We are interested in knowing the extent to which a given combinatorial property of permutation groups depends on group theoretic properties. Said another way, suppose we are given a property P of permutation groups. (1) What abstract groups can be realized as permutation groups having property P? And, (2) given an abstract group G and a property P, can we find all possible realizations of G as a permutation group possessing property P?

When P is the property of transitivity, we can answer question (1). Cayley showed that every group is isomorphic to a permutation group. His proof amounted to a construction of the regular representation of an arbitrary group. Since the regular representation is transitive, *every group can be realized as a transitive permutation group.*

In this expository paper, we are interested in letting P be the property of double transitivity. Most of the results we will develop are old. Our purpose is to bring them together for an attack on questions (1) and (2).

Of course, doubly transitive groups are transitive. We shall begin by answering question (2) when $P=$ transitivity.

2. Transitive Representations

Let G be an abstract group with subgroup H. Let $\mathscr{H}=\{x_1H, x_2H, \ldots, x_mH\}$ be the set of distinct left cosets of H in G, where $m=[G:H]$. Then G acts on $\mathscr{H}$ (written $G:\mathscr{H}$) as follows: If $g \in G$ then

AMS (1971) Subject Classification: Primary 2020, Secondary 2025, 2040, 2080.

*An invited paper.

**Present address: Department of Mathematics, California State College, Hayward, Calif. 94542.

$g(x_iH)=gx_iH$ for $1 \leqslant i \leqslant m$. Clearly, G permutes the elements of $\mathscr{H}$ among themselves. Thus, G acts as a permutation group on the elements of $\mathscr{H}$. Observe that $x_jx_i^{-1}(x_iH)=x_jH$ so that $G{:}\mathscr{H}$ transitively. We say that this permutation representation of G **corresponds** to the subgroup H.

Suppose now that G is a permutation group acting transitively on $A=\{a=a_1, a_2,\ldots,a_m\}$. Let H be the subgroup of G which fixes the element a, i.e., $g \in G$ is in H if and only if $g(a)=a$. (We will sometimes write G_a for this subgroup.) Let $x_2, x_3,\ldots, x_m$ be elements of G such that $x_ia_1=a_i$, $2 \leqslant i \leqslant m$. Then it is easily verified that $\mathscr{H}=\{H, x_2H,\ldots, x_mH\}$ is the set of distinct left cosets of H in G. (Indeed, $m=[G{:}G_a]$ if and only if G acts transitively on A.)

We have established a one-to-one correspondence between the elements of A and the elements of $\mathscr{H}$. It is easily verified that the action of G on A is carried over by this correspondence to the action of G on $\mathscr{H}$ described previously. It follows that *every transitive permutation representation of an abstract group* G *corresponds to some subgroup* H. We remark that the representation of G corresponding to $\{e\}$ is the regular representation.

DEFINITION. Let H and K be subgroups of G. We say $G{:}\mathscr{H}$ and $G{:}\mathscr{K}$ in *essentially the same way* if there exists a one-to-one function f from $\mathscr{H}$ onto $\mathscr{K}$ such that $fg(a)=gf(a)$ for all $g \in G$ and $a \in \mathscr{H}$.

It is easily seen that $G{:}\mathscr{H}$ and $G{:}\mathscr{K}$ in essentially the same way if and only if H is conjugate to K in G.

We now consider the faithfulness of the representation $G{:}\mathscr{H}$. Let $g \in G$ be such that $gxH=xH$ for every $x \in G$. Then $x^{-1}gx \in H$, or $g \in xHx^{-1}$ for every $x \in G$. Thus, the kernel of the representation $G \rightarrow G{:}\mathscr{H}$ is $K=\bigcap_{x\in G} xHx^{-1}$. Clearly, K is normal in G. Of the subgroups of H which are normal in G, K is the unique maximal one. In particular, the representation $G \rightarrow G{:}\mathscr{H}$ is faithful if and only if H contains no subgroup $K \neq \{e\}$ which is normal in G. It follows immediately that if G is abelian then $G \rightarrow G{:}\mathscr{H}$ is faithful if and only if $H=\{e\}$, i.e., *the regular representation is the only faithful transitive permutation representation of an abelian group.*

3. Doubly Transitive Representations

We begin this section by disposing of a troublesome exceptional case. Suppose G has a subgroup H of index 2. It is a standard exercise to show that H is normal. Thus, the representation of G corresponding to H is of **degree** 2 (i.e., it is subgroup of S_2) and the representation group is of order 2. Therefore, the action of G on $\mathscr{H}$ must be doubly transitive.

Let G be a doubly transitive permutation group. Suppose $G{:}A$, i.e., G is a group of one-to-one functions from A onto A. As before, let G_a be the subgroup of G which fixes $a \in A$. Since G is doubly transitive on A, G_a must be transitive on $A \setminus \{a\}$. Conversely, suppose G_a is transitive on $A \setminus \{a\}$ for all $a \in A$. (We rule out the case that the cardinality of A, $|A|$, is 1.) Given two pairs of elements from A, (a_1, a_2) and (b_1, b_2) such that $a_1 \neq a_2$ and $b_1 \neq b_2$, we seek a $g \in G$ such that $g(a_1)=b_1$ and $g(a_2)=b_2$.

If there exists an $a \in A$ which is neither a_1 nor b_1 then by hypothesis, there exists a $g_1 \in G_a$ such that $g_1(a_1)=b_1$. Now, since $a_2 \neq a_1$, it follows that $g_1(a_2) \neq b_1$. But, also, $b_2 \neq b_1$. Hence, there is a $g_2 \in G_{b_1}$ such that $g_2(g_1(a_2))=b_2$. It follows that we may take $g=g_2g_1$.

But, if $|A| \geqslant 3$, such an a always exists. (If $|A|=2$, it may not, e.g., $G=\{e\}$ and $|A|=2$ gives rise to the unpleasant situation in which G_a is transitive on $\mathrm{A}\setminus\{a\}$ for all $a \in A$ but G is not doubly transitive.) We have proved our first result.

THEOREM 1: *Suppose* $\mathrm{G{:}A}$. *If* $|\mathrm{A}| \geqslant 3$ *then* $\mathrm{G{:}A}$ *doubly transitively if and only if* $\mathrm{G_a}$ *acts transitively on* $\mathrm{A} \setminus \{\mathrm{a}\}$ *for every* $\mathrm{a} \in \mathrm{A}$.

If we are willing to assume in the previous argument that $G{:}A$ transitively, we may simply choose $g_1 \in G$ such that $g_1(a_1)=b_1$. Thus, we have another version of theorem 1.

THEOREM 1′: *Assume* $\mathrm{G{:}A}$ *transitively. If* $|\mathrm{A}| \geqslant 2$, *then* $\mathrm{G{:}A}$ *doubly transitively if and only if* $\mathrm{G_a}$ *acts transitively on* $\mathrm{A} \setminus \{\mathrm{a}\}$ *for any* $\mathrm{a} \in \mathrm{A}$.

Indeed, it is easy to see that transitivity implies that $G_a{:}A \setminus \{a\}$ transitively for any $a \in A$ if and only if it acts transitively for every $a \in A$. Theorem 1′ is the version most often encountered in books, e.g., Passman [7, p. 16],[1] Ledermann [5, p. 85], and Wielandt [9, p. 19].

COROLLARY 1: ([1, p. 177], [5, p. 85], [9, p. 20]). *Suppose* $G{:}A$ *doubly transitively. Let* $|A| = m$. *Then* $m(m-1)$ *divides* $|G|$.

PROOF: We have seen in section 2 that $m = [G{:}G_a]$ for any $a \in A$. By Theorem 1′, $m - 1 = [G_a{:}G_a \cap G_b]$ for any distinct pair $a, b \in A$. Hence, $[G{:}G_a \cap G_b] = [G{:}G_a][G_a{:}G_a \cap G_b] = m(m-1)$.

Q.E.D.

Now, if G is an abstract group with a doubly transitive representation $G{:}\mathscr{H}$ corresponding to H, then $m = [G{:}H]$ and $m(m-1)$ divides $[G{:}K]$ where K is the kernel of the representation. Hence, certainly, $m(m-1)$ divides $|G|$. *In particular,* $|G|$ *must be even.*

One might ask if there are doubly transitive groups $G{:}A$ where $|A| = m =$ the degree of G and $|G| = m(m-1)$. Burnside [1, §140] has shown that such a group exists if and only if m is a power of a prime.

THEOREM 2: *If* $G{:}\mathscr{H}$ *doubly transitively then* $H = N(H)$, *the normalizer of* H *in* G, *or* $[G{:}H] = 2$.

PROOF: Suppose $g \in N(H) \setminus H$. Then $gH \in \mathscr{H}$, and $gH \neq H$. Now, $H \subset G$ is the stabilizer of $H \in \mathscr{H}$, i.e., $xH = H$ if and only if $x \in H$. By Theorem 1′ , H must act transitively on $\mathscr{H} \setminus \{H\}$. But since $g \in N(H)$, we have that $hgH = gH$ for all $h \in H$. We have reached a contradiction unless $[G{:}H] = 2$, in which case $\mathscr{H} \setminus \{H\} = \{gH\}$.

COROLLARY 2: *Suppose* $G{:}\mathscr{H}$ *doubly transitively. If* G *is nilpotent then* $[G{:}H] = 2$.

PROOF: By Hall [3, Theorems 4.3.3 and 10.3.4] we may make the following definition: G is **nilpotent** if no proper subgroup of G is its own normalizer in G. The result follows from Theorem 2.

(In spite of Corollary 1 ruling out groups of odd order and Corollary 2 eliminating nilpotent groups except in the trivial case, there are solvable doubly transitive groups. The group of even permutations on four letters, A_4, is solvable.)

COROLLARY 3: *If the center of* G, $Z(G)$, *is not the identity alone, then* G *has a faithful representation as a doubly transitive permutation group if and only if* $|G| = 2$.

Let H be a subgroup of G. If $Z(G) \cap H \neq \{e\}$ then the representation corresponding to H cannot be faithful. If $Z(G) \not\subset H$ then $Z(G) \setminus H \subset N(H) \setminus H$. Thus $H \neq N(H)$.

THEOREM 3: *Suppose* $G{:}\mathscr{H}$ *doubly transitively. Then* H *is a maximal subgroup of* G.

PROOF: Let K be the kernel of the representation $G \rightarrow G{:}\mathscr{H}$. Via the usual isomorphism, $(G/K){:}\mathscr{H}$ doubly transitively. By [7, p. 18] $(G/K){:}\mathscr{H}$, being doubly transitive, is primitive. By [7, p. 15] we may take as our definition of primitivity that H/K is maximal in G/K. Thus H is maximal in G.

(If G is to have a faithful representation as a permutation group on m letters then $|G|$ must divide m, the order of S_m. In particular, if the representation corresponds to H then $|G|$ divides $[G{:}H]!$. By the previous theorem, when $G{:}\mathscr{H}$ doubly transitively, $[G{:}H]$ is likely to be "small" compared with $|G|$.)

We are now going to use Theorem 1′ together with the discussion of §2 to obtain some necessary and sufficient conditions that the representation of G corresponding to H be doubly transitive. Again, take $\mathscr{H} = \{x_1H, \ldots, x_mH\}$, but now assume that $x_1 \in H$. To prove that $G{:}\mathscr{H}$ doubly transitively, we need only show the existence of $h_2, \ldots, h_m \in H$ such that $h_i x_2 H = x_i H$, $2 \leqslant i \leqslant m$. Hence, we have the following result.

THEOREM 4: [7, p. 17]. *The representation of* G *corresponding to* H *is doubly transitive if and only if* $G \setminus H = HgH$ *for any / every* $g \in G \setminus H$.

COROLLARY 4: *The representation of* G *corresponding to* H *is doubly transitive if and only if* $[G{:}H] = [H{:}g^{-1}Hg \cap H] + 1$ *for any / every* $g \in G \setminus H$.

PROOF: According to Hall [3, Theorem 1.7.1], the number of left cosets in the "double coset" HgH is $[H{:}g^{-1}Hg \cap H]$. According to Theorem 4, $G{:}\mathscr{H}$ doubly transitively if and only if this number is $[G{:}H] - 1$.

(Corollary 4 also follows from the proof of corollary 1.)

One immediate consequence of Corollary 4 is that $([G{:}H] - 1)$ divides the order of H.

[1] Figures in brackets indicate the literature references at the end of this paper.

Before we proceed to the next result it will be convenient to define a **proper coset** of H in G as a coset of H in G which is not a subgroup of G, i.e., xH is a proper coset if and only if $x \notin H$.

COROLLARY 5: *The representation of* G *corresponding to* H *is doubly transitive if and only if for any / every* $g \in G \setminus H$, *a system of representatives for the proper left cosets of* H *in* G *may be chosen from the right coset* Hg.

PROOF: Suppose $G{:}\mathscr{H}$ doubly transitively. Let $g \in G \setminus H$. By Theorem 4, $HgH = G \setminus H$. Thus, there exist $e = h_2, h_3, \ldots, h_m \in H$ such that $\mathscr{H} = \{H, h_2gH, h_3gH, \ldots, h_mgH\}$. But, $h_ig \in Hg$, $2 \leqslant i \leqslant m$.

Conversely, suppose $\mathscr{H} = \{H, x_2H, \ldots, x_mH\}$ and $x_2, \ldots, x_m \in Hx$ for some $x \in G \setminus H$. Then $Hx_2 = \ldots = Hx_m$. Let $x_ix_2^{-1} = h_i \in H$, for $2 \leqslant i \leqslant m$. Then $x_i = h_ix_2$ and $x_iH = h_ix_2H$. Thus $x_iH \subset Hx_2H$, for $2 \leqslant i \leqslant m$. The result follows from Theorem 4.

It is interesting to compare Corollary 5 with the following combinatorial result:

THEOREM [8, p. 51]. *Let* G *be a finite group and let* H *be a subgroup of* G. *There exist elements* $g_1, g_2, \ldots, g_m$ *in* G *such that*

$$G = Hg_1 \cup \ldots \cup Hg_m = g_1H \cup \ldots \cup g_mH,$$

where $m = [G{:}H]$.

COROLLARY 6. *If the commutator subgroup of* G *is contained in* H *and if* $[G{:}H] > 2$, *then the representation of* G *corresponding to* H *cannot be doubly transitive.*

PROOF. Suppose C_1 and C_2 are two different proper left cosets of H in G. Suppose $G{:}\mathscr{H}$ doubly transitively. By Corollary 5, there exist $x, y \in G$ such that $xH = C_1$, $yH = C_2$, and $xy^{-1} \in H$. If the commutator $z = yx^{-1}y^{-1}x \in H$ then $y^{-1}x \in xy^{-1}H = H$, which is impossible since $xH \neq yH$.

4. Matrix Representations

There are many ways of expressing the elements of a permutation group. Let $A = \{1, 2, \ldots, m\}$ and suppose $G{:}A$. We wish to represent $g \in G$ by the m-square matrix $P(g)$ whose i, j entry is 1 if $i = g(j)$ and 0 otherwise. It is easy to see that $P(e) = I$, the m-square identity matrix, and $P(g_1g_2) = P(g_1)P(g_2)$ for all $g_1, g_2 \in G$. It follows that $g \rightarrow P(g)$ in a representation in the ordinary sense of group representation theory. (If we let e_i be the $1 \times m$ column vector with a 1 in row i and 0 elsewhere, $\{P(g){:}g \in G\}{:}\{e_i{:}1 \leqslant i \leqslant m\}$ is "permutation isomorphic" to $G{:}A$.)

Suppose $G{:}A$. For $g \in G$, let $\theta(g)$ be the number of points (elements) of A fixed by g. Then $\theta(g)$ is the cardinality of $\{a \in A{:}g(a) = a\}$. Clearly $\theta(g)$ is the trace of $P(g)$. Thus θ is a character on G.

Before we can prove our next theorem, we need to do some preliminary work. Let $a, b \in A$. We say $\mathbf{a \equiv b (mod\ G)}$ if there is a $g \in G$ such that $g(a) = b$. Because of the group properties, $\equiv$ (mod G) is easily seen to be an equivalence relation. The equivalence classes in A induced by $\equiv$ (mod G) are called **orbits** of G. In particular, $G{:}A$ transitively if and only if A is the only orbit of G. If $O \subseteq A$ is an orbit of G, then it makes sense to write $G{:}O$. Of course, $G{:}O$ transitively.

LEMMA ([7, p. 13], [1, p. 191], [9, Exercise 3.10]). *Let* t *be the number of orbits of* G *in* A. *Then*

$$\sum_{g \in G} \theta(g) = t|G|.$$

PROOF: We count the set $S = \{(g,a){:}a \in A \text{ and } g \in G_a\}$ in two ways:

$$\sum_{g \in G} \theta(g) = \sum_{a \in A} |G_a|.$$

It is an easy exercise to verify that $[G{:}G_a]$ is the number of elements in the orbit of G to which a belongs. Thus

$$\sum_{a \in A} |G_a| = t|G| \tag{1}$$

THEOREM 5: *Suppose* G:A *where* $|A| \geqslant 2$. *Then*

$$|G|^{-1}\sum_{g\in G}\theta(g)^2\geqslant 2$$

with equality if and only if G:A *doubly transitively.*

(Most books, e.g., [1, p. 191], [3, Theorem 16.6.14], and [7, Proposition 3.9], hypothesize that G be transitive in Theorem 5. As we shall see, this is unnecessary.)

PROOF: Following Passman [7, p. 18], we count the set $S=\{(g,a,b):a,b,\in A, g\in G_a\cap G_b\}$ in two ways. For fixed $g\in G$, there are $\theta(g)$ possibilities for a and $\theta(g)$ possibilities for b (we may have $a=b$). Thus $|S|=\Sigma\theta(g)^2$. For fixed b, there are $\theta(g)$ possibilities for a where g is allowed to range over G_b. Thus

$$|S|=\sum_{b\in A}\sum_{g\in G_b}\theta(g)$$

$$=\sum_{b\in A}t_b\,|\,G_b\,|,$$

by the lemma, where t_b is the number of orbits of G_b acting on A. Since G_b fixes b and $|\,A\,|\geqslant 2, t_b\geqslant 2$. Moreover, $t_b=2$ if and only if G_b is transitive on $A\setminus\{b\}$. Thus

$$|S|\geqslant 2\sum_{b\in A}|G_b| \tag{2}$$

with equality if and only if G_b is transitive on $A\setminus\{b\}$ for all $b\in A$. But, from (1),

$$\sum_{b\in A}|G_b|=t\,|\,G\,|$$

where t is the number of orbits of G in A. Hence, $|S|\geqslant 2t|G|\geqslant 2|G|$.

Suppose $|S|=2|G|$. Then $t=1$ meaning that G is transitive. But, we must also have equality in (2). Using Theorem 1′ we conclude that $|S|=2|G|$ if and only if G is doubly transitive. Q.E.D.

Since θ is a real character, one recognizes that the left hand side of the inequality in Theorem 5 is, by the orthogonality relations for characters, the sum of the squares of the multiplicities of the irreducible characters belonging to θ. We have proved our next result.

COROLLARY 7 ([2, Theorem 32.5], [3, Theorem 16.6.15]): *Let* G : A. *The representation* g→ P(g) *reduces into at least two irreducible pieces, one of which is the identically* 1 *representation. It reduces into exactly two* pieces *if and only if* G:A *doubly transitively.*

Thus, if G is an abstract group with a faithful representation as a doubly transitive group, G has a faithful irreducible representation. This brings us to the following question: What abstract groups, G, have faithful irreducible representations? It is not hard to show that G must have a cyclic center. But, there exist groups having trivial center which do not have faithful irreducible representations. Burnside [1, p. 476] gives such a group of order 18. He also gives a sufficient condition that G have a faithful irreducible representation. Weisner [6, p. 68] has given a necessary and sufficient condition that G have a faithful irreducible representation. Other work on this question has been done by Kochendörffer [4].

Now, suppose one has an irreducible representation, $g\rightarrow R(g)$ of an abstract group G. When does there exist a nonsingular matrix U such that

$$\mathrm{U}^{-1}\begin{bmatrix}1 & 0\\ 0 & R(g)\end{bmatrix}\mathrm{U}=P(g) \tag{3}$$

is a permutation matrix for every $g\in G$? Of course, if such a U exists then $g\rightarrow P(g)$ is a doubly transitive representation of G. Certainly it is necessary that trace $R(g)$ be an integer $\geqslant -1$ for every

g. Also, except when G has a subgroup of index 2, trace $R(e)$ must be greater than 1. But, these simple conditions are not sufficient. The nonabelian group G of order 14 has a faithful irreducible representation $g \rightarrow R(g)$ of degree $(=R(e))$ three such that trace $R(g)$ is an integer greater than or equal to -1 for all $g \in G$. If it were possible to satisfy (3) for this group and representation then G would have a faithful representation as a doubly transitive group. But this would contradict corollary 1, since there is no integer m such that $m(m-1)$ divides 14.

5. Other Results

Hardly an issue of *Mathematical Reviews* goes by without some mention of double transitivity. Transitivity properties are among the most interesting from the fruitful and durable field of permutation groups. Interesting results beyond those which have been given here abound; but the methods are not elementary. Since he has raised the question of solvability, however, the author cannot resist including one last remark without proof, one which is perhaps illustrative of current work. Burnside [1, p. 341] has "shewn" that a *simply transitive* (transitive but not doubly transitive) group of prime degree p is of order pq where q is a prime factor of $p-1$. Since groups of order pq are solvable, it follows [9, p. 29] that *every nonsolvable transitive group of prime degree is doubly transitive.*

6. References

[1] Burnside, W., Theory of Groups of Finite Order, (Dover, New York, 1955).

[2] Curtis, C., and Reiner, I., Representation Theory of Finite Groups and Associative Algebras, (Interscience, New York, 1962).

[3] Hall, M., Jr., The Theory of Groups, (Macmillan, New York, 1959).

[4] Kochendörffer, R., Über treue irreduzible Darstellungen endlicher Gruppen, Math. Nachrichten **1**, 25–39 (1948).

[5] Ledermann, W., Introduction to the Theory of Finite Groups, (Interscience, New York, 1957).

[6] Lomont, J. S., Applications of Finite Groups, (Academic Press, New York, 1959).

[7] Passman, D., Permutation Groups, (Benjamin, New York, 1968).

[8] Ryser, H. J., Combinatorial Mathematics, carus Mathematical Monograph number 14, (Wiley, New York, 1963).

[9] Wielandt, H., Finite Permutation Groups, (Academic Press, New York, 1964).

[10] Zassenhaus, H., The Theory of Groups, second edition, (Chelsea, New York, 1958).

(Paper 76B1&2–360)