A SIMPLE GROUP HAVING NO MULTIPLY TRANSITIVE REPRESENTATION

E. T. PARKER

The totality of 4×4 matrices with coefficients in $GF\ [2^2]$, determinant unity, and which permute among themselves the vectors of dimension 4 having 4 co-ordinates nonzero marks of $GF\ [2^2]$, or 2 zeros and 2 nonzero marks of the field, forms a simple [**1**, p. 285, problem 9, part (4)][1] (multiplicative) group, G, of order $2^6 \cdot 3^4 \cdot 5$. It will be demonstrated that G is isomorphic with no multiply transitive permutation group.

After submitting the manuscript, the author received a communication, quoted in part, "The referee has observed that if one is willing to use Frame's table (Duke Math. J. vol. 2) for the characters of this group, then the result can be derived in a few lines as follows. The degrees of the irreducible representations are 1, 5, 6, 10, 15, 20, 24, 30, 40, 45, 60, 64, 81. If the group had a doubly transitive permutation representation of degree n, then n would divide the order of the group and $n-1$ would be a degree of an irreducible representation. Moreover, the character of this irreducible representation has to be rational and its values must be $\geqq -1$. This eliminates all degrees except $n-1=15$. However, the character in question has the value 3 for an element of order 4 and values -1 for all elements of order 2. This would mean that the element of order 4 leaves 4 letters fixed while its square changes all letters."

In the remainder of the paper the counter-example will be established independently of characters:

In order that G be representable as at least doubly transitive on n symbols, it is necessary that $n! \geqq 2^6 \cdot 3^4 \cdot 5$, and $n(n-1)$ be a divisor [**1**, p. 141, Theorem II] of $2^6 \cdot 3^4 \cdot 5$. Thus n must be 9, 10, 16, or 81.

The cases 9 and 10 are easily disposed of, for 10! is divisible by only the fourth power of 3. Hence, if G were represented on 9 or 10 symbols, then each of its Sylow subgroups belonging to 3 must be a Sylow subgroup of the symmetric group; such a subgroup contains a cycle of 3 symbols, which generates a primitive group of degree 3. But a doubly transitive [**1**, p. 160] group is primitive; and a primitive [**3**, p. 92, Theorem II] group of degree n containing a primitive subgroup of degree m is at least $(n-m+1)$-fold transitive. This is the desired contradiction.

Received by the editors April 20, 1951 and, in revised form, December 10, 1953.

[1] In problem 10 following, Carmichael implicitly raises the question settled in this paper. For a more general treatment, see [**2**, pp. 126–138].

Those matrices of G having only one nonzero mark in each column (and consequently in each row) form a subgroup P of order $4!\cdot 3^4/3 = 2^3\cdot 3^4$. Each of these matrices is the product of a matrix x in P having one 1 and three zeros in each column ("permutation matrix"), and a matrix y in P with nonzero marks only on its principal diagonal ("diagonal matrix"). If the unit in the ith row of x is in its jth column, then the (i, i)th entry of any 4×4 matrix, c, (with coefficients in the field) becomes the (i, j)th of cx, and in turn the (j, j)th of $x^{-1}cx$. (The row index is written first.) In particular, c and $x^{-1}cx$ have the same totality of marks on their principal diagonals. Also, c and $y^{-1}cy$ have the same *sequence* of marks on their diagonals, for the conjugation consists of multiplying each column of c by a nonzero mark, and the corresponding row of c by the reciprocal of that mark. Thus, if p is a matrix of P, then c and $p^{-1}cp$ have the same totality of marks on their diagonals.

$$t = \begin{bmatrix} 1 & 1+a & a & 0 \\ 0 & 1+a & a & 1 \\ a & 1 & 0 & a \\ 1+a & 0 & 1 & 1+a \end{bmatrix}$$

and

$$t^{-1} = \begin{bmatrix} 1 & 0 & 1+a & a \\ a & a & 1 & 0 \\ 1+a & 1+a & 0 & 1 \\ 0 & 1 & 1+a & a \end{bmatrix}$$

where "a" designates a primitive mark of $GF[2^2]$, are inverse elements of G of order 5. Since t and t^{-1} have distinct totalities of marks on their principal diagonals, they are conjugate under no matrix of P. And t is not conjugable into t^2 under a matrix p of P; for it would follow that $(p^2)^{-1}t(p^2) = t^{2^2} = t^4 = t^{-1}$, where p^2 is in the subgroup P. Similarly, t cannot be conjugated into t^3 under any matrix of P.

Assume that t is permutable with a matrix p of P, and set $p = xy$. In order that t and $x^{-1}tx$ have the same sequence of marks on their principal diagonals, it is necessary that x be the identity matrix or

$$x_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Conjugation of a matrix c by a diagonal matrix y of P can replace no zero of c by a nonzero mark in the same position, or vice versa. t and $x_1^{-1}tx_1$ have distinct patterns of zeros; hence, x can be chosen as only the identity matrix. Now, it is readily seen that if $p=y$, then $p^{-1}tp\neq t$ unless the four diagonal marks of p are equal; that is, $p=$identity, since all matrices of G have determinant unity.

It has been established that the conjugate of t by each nonidentical matrix of P is an element of G not in the subgroup generated by t. If p_1 and p_2 are distinct matrices of P, then $p_1^{-1}tp_1$ and $p_2^{-1}tp_2$ do not belong to a common subgroup of order 5; for this would imply that $(p_1p_2^{-1})^{-1}t(p_1p_2^{-1})$ is a power of t, where $p_1p_2^{-1}$ is a nonidentical element of the subgroup P.

It follows now that G has at least as many Sylow subgroups of order 5 as P has elements, namely $2^3\cdot 3^4$. The only divisor [**4**, p. 67, Theorem 74] of $2^6\cdot 3^4\cdot 5$ which is $\geqq 2^3\cdot 3^4$ and $\equiv 1 \pmod 5$ is $2^4\cdot 3^4$. Hence, G has $2^4\cdot 3^4$ Sylow subgroups of order 5; each has a normalizer [**4**, p. 67, Theorem 74] in G of order $5\cdot 4$.

$$s = \begin{bmatrix} a & 1+a & 0 & 1+a \\ 1+a & a & 0 & 1+a \\ 1+a & 1+a & 0 & a \\ 0 & 0 & 1+a & 0 \end{bmatrix}$$

is an element of G such that $s^{-1}ts=t^2$. Thus the normalizer in G of a Sylow subgroup of order 5 is isomorphic with the metacyclic [**1**, p. 184, exercise 10] group of order 20.

Now, if G is representable transitively [**1**, p. 157, Theorem XII] on 16 symbols, it must have a subgroup H of index 16—order $2^2\cdot 3^4\cdot 5$. Since the order of the normalizer in G of a Sylow subgroup of order 5 is not divisible by 3, the only possibility [**4**, p. 67, Theorem 74] is that H have 81 subgroups of order 5; and the normalizer of each H must be of order 20, accordingly isomorphic with the metacyclic group. Hence H has elements of order 4, and its Sylow subgroups belonging to 2 are cyclic. The cyclic group of order 4 has only one nonidentical automorphism [**1**, p. 104]; this is of order 2. The normalizer [**4**, p. 67, Theorem 73] of a Sylow subgroup contains no elements of order a power of that prime, except those in the Sylow subgroup. Hence, each Sylow subgroup of order 4 is in the central of its normalizer in H. By a theorem of Burnside [**4**, p. 141, Theorem 122], the commutator-subgroup, H_1, of H is of order prime to 2. H_1 is of order divisible by at most two distinct primes, and is therefore solvable [**1**, p. 229, Corollary 2]. The sequence of commutator-subgroups of H

terminates in the identity [4, p. 43, Theorem 36], and H is solvable.

Since the normalizer [4, p. 67, Theorem 73] of a Sylow subgroup contains only the one subgroup of that order, H must have a conjugate class of 81 subgroups isomorphic with the metacyclic group of order 20. No pair [4, p. 67, Theorem 73] of these can have a subgroup of order 5 in common; hence their intersection is of order at most 4. And since this metacyclic group has no normal subgroup of order 2 or 4, a subgroup of order 20 of H is neither normal under H, nor contains a nonidentical normal subgroup of H. Hence H must be isomorphic with a transitive [1, p. 157, Theorem XII] group of degree 81. If H' is a subgroup of H containing one of the subgroups of order 20, then the normalizer in H' of a subgroup of order 5 is of order at least 20; and at most 20, for this is the order of the normalizer in G of a Sylow subgroup of order 5. The index under H' of this normalizer is the number of Sylow subgroups of order 5 in H'; since this number can be no power of 3 between 1 and 81, each subgroup of order 20 must be a maximal subgroup of H. Hence, the representation of H on 81 symbols is primitive [1, p. 160, Theorem XIV]. A normal subgroup ($\neq$identity) of a primitive group is transitive on all the symbols [1, p. 163, exercise 13]. Accordingly, each normal subgroup ($\neq$identity) of H is of order divisible [1, p. 141, Theorem II] by 81. As shown above, H must be solvable; and a solvable group has a normal elementary [4, p. 41, Theorem 31] subgroup ($\neq$identity). The only prime-power divisible by 3^4, and itself a divisor of the order of H, is 3^4. But G has no elementary subgroup of order 3^4; its subgroups of this order are Sylow subgroups, one of which contains [4, p. 65, Theorem 68] the following element of G of order 3^2:

$$\begin{bmatrix} a & 0 & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

If G is isomorphic with a transitive group of degree 81, then G must have a subgroup [1, p. 157, Theorem XII] K of index 81—order $2^6 \cdot 5$. K must have 2^4 subgroups of order 5 with their normalizers isomorphic with the metacyclic group of order 20. Repeating arguments of the preceding paragraph, K must be isomorphic with a primitive group of degree 16. K is solvable [1, p. 229, Corollary II]; thus it must have a normal elementary subgroup A transitive on the 16 symbols. A can be of order only 16, for a commutative transitive group is regular [1, p. 155, Theorem XI]. The subgroup K' of K, with one of the 16 symbols fixed [1, p. 142, Corollary III], is of order 20, and therefore isomorphic with the metacyclic group. An element r of order 4 in K' leaves fixed at least one of the 16 symbols; hence r^2 does likewise. r^2 is not an element of A, for each nonidentical element of A is regular on the 16 symbols, nor is r^2 permutable with each element of A, for then $\{A, r^2\}$ would be a commutative [1, p. 155, Theorem XI] group of order $>2^4$, but transitive on 2^4 symbols. Thus, conjugation of K by r^2 induces a nonidentical automorphism of A; and conjugation by r an automorphism of A of order 4. $\{A, r\}$ is a subgroup of order 2^6 of K and $\{A, r\}/A$ is cyclic. It will be shown that the Sylow subgroups of this order in G are not of this structure.

$$\alpha_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad \alpha_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\alpha_3 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \quad \text{and} \quad \alpha_4 = \begin{bmatrix} 0 & 1 & a & a \\ 1 & 0 & a & a \\ 1+a & 1+a & 0 & 1 \\ 1+a & 1+a & 1 & 0 \end{bmatrix}$$

are matrices of G. Each is of order two, each pair is permutable, and the four are independent (since the first two are permutations, but not the third, and the first three have all entries 0 or 1, but not the last). Thus the four generate an elementary group N of order 2^4.

$$\beta = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \gamma = \begin{bmatrix} 0 & 1+a & 1+a & 1 \\ a & 1 & 0 & a \\ a & 0 & 1 & a \\ 1 & 1+a & 1+a & 0 \end{bmatrix}$$

are also elements of G of order 2. $\beta^{-1}N\beta = N$ and $\gamma^{-1}N\gamma = N$. $(\beta\gamma)^2 = \alpha_3$; therefore, since β and γ are each of order only 2, N has at most 4 cosets (including itself) in $\{N, \beta, \gamma\}$. Conjugation of N by β effects the automorphism, expressed as a permutation (for example, $\alpha_1\alpha_4$ is written below as "14"):

$$(1, 2)\ (4, 1234)\ (13, 23)\ (34, 124)\ (24, 234)\ (14, 134).$$

And conjugation of N by γ yields:

$$(1, 4)\ (2, 1234)\ (13, 34)\ (23, 124)\ (24, 234)\ (12, 123).$$

Since the above permutations are distinct, and neither is the identity, the four cosets of N are all distinct, and $S = \{N, \beta, \gamma\}$ is of order 2^6; that is, S is one of the Sylow subgroups belonging to 2 of G. S/N is isomorphic with the *elementary* group of order 4. It may be noted that the permutations are permutable, and that their product is similar to either.

It remains to be shown that S does not have a normal elementary subgroup of order 2^4 with *cyclic* quotient-group relative to S. It will be demonstrated that, besides N, S has no commutative subgroup of order 2^4. A subgroup of index 4 in S must have an intersection [**4**, p. 63, Theorem 65] of order at least 4 with N, and of order at least 8 with each of $\{N, \beta\}$, $\{N, \gamma\}$, $\{N, \beta\gamma\}$. If the intersection with N is of order 4, then the intersection with each of $N\beta$, $N\gamma$, and $N\beta\gamma$ consists of 4 elements. But only two elements (identity and α_3) of N are permutable with both $\beta\alpha$ and $\gamma\alpha'$, where α and α' are elements of N. And if the intersection with N is of order 8, then the intersection with one of $N\beta$, $N\gamma$, or $N\beta\gamma$ consists of 8 elements. But only four elements of N are permutable with $\beta\alpha$, $\gamma\alpha$, or $\beta\gamma\alpha$.

Bibliography

1. R. D. Carmichael, *Introduction to the theory of groups of finite order*, New York, Ginn, 1937.

2. L. E. Dickson, *Linear groups with an exposition of Galois field theory*, Leipzig, Teubner, 1901.

3. W. A. Manning, *Primitive groups*, Stanford University Press, 1921.

4. A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, New York, Dover, 1943.

University of Texas